S. Hrg. 107–205

HOW SECURE IS OUR CRITICAL INFRASTRUCTURE?

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

SEPTEMBER 12, 2001

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

76–799 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	FRED THOMPSON, Tennessee
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
RICHARD J. DURBIN, Illinois	SUSAN M. COLLINS, Maine
ROBERT G. TORRICELLI, New Jersey	GEORGE V. VOINOVICH, Ohio
MAX CLELAND, Georgia	PETE V. DOMENICI, New Mexico
THOMAS R. CARPER, Delaware	THAD COCHRAN, Mississippi
JEAN CARNAHAN, Missouri	ROBERT F. BENNETT, Utah
MARK DAYTON, Minnesota	JIM BUNNING, Kentucky

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
JINNETT RONA-FINLEY, *Detailee, CIA*
KIERSTEN TODT COON, *Congressional Fellow for Senator Lieberman*
HANNAH S. SISTARE, *Minority Staff Director and Counsel*
ELLEN B. BROWN, *Minority Senior Counsel*
ROBERT J. SHEA, *Minority Counsel*
MORGAN P. MUCHNICK, *Minority Professional Staff Member*
DARLA D. CASSELL, *Chief Clerk*

CONTENTS

WITNESSES

WEDNESDAY, SEPTEMBER 12, 2001

ALPHABETICAL LIST OF WITNESSES

APPENDIX

HOW SECURE IS OUR CRITICAL INFRASTRUCTURE?

WEDNESDAY, SEPTEMBER 12, 2001

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 11:06 a.m., in room SH–216, Hart Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Thompson, Levin, Bennett, Dayton, Bunning, and Carper.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. This morning, the Senate Governmental Affairs Committee will proceed with its previously scheduled hearing—the first in what we expect to be a series of hearings and investigations on a problem that is today even more important to us than before—the security of our critical infrastructure and the vulnerability of our homeland to unconventional enemy attack.

The attacks yesterday struck many individual families and the broader American family. I pause for a moment here at the outset of this hearing to indicate that it also struck the family of the Senate Governmental Affairs Committee. Barbara Olson, who was killed on one of the planes yesterday, had served as an assistant to Senator Nickles for some period of time in his work on this Committee. On behalf of the entire Committee, I extend my condolences to her husband and her family and want them to know that they are in our prayers.

Today, we do consider critical infrastructure to be a vast array of elements that form the backbone of America. The critical infrastructure is, in essence, our Nation's skeleton, the framework underlying our well-being and our freedom. It includes telecommunications systems, air traffic control systems, electricity grids, emergency and law enforcement services, water supplies, financial networks, and energy pipelines.

Today, our hearts and minds are naturally focused on yesterday's tragedy, but it is important that the Senate continue with America's business, particularly as it affects America's security. Thus, we are holding this hearing as originally planned, with the same focus that we had intended, which is to explore the extent to which our critical infrastructure is vulnerable, particularly to manipulations and attacks from cyberspace, the consequences of that vulnerability and what the government is doing and must do to reduce

that vulnerability. For as we saw tragically yesterday, our enemies will increasingly strike this mighty Nation at places where they believe we are not only dependent but we are unguarded. And that is surely true of our cyberspace infrastructure today.

More and more we find that everything in our lives is being operated by a computer system, from Wall Street to Main Street. Where once our economy was dependent primarily on the movement of goods and services by road or rail, the products and services of our new economy are now just as likely to travel via the Internet as they are to move on an interstate.

While it has never been easy to protect all of our critical infrastructure from conventional attacks—and, of course, they have happened only rarely in our history here at home—it has become even more difficult now to safeguard our Nation from cyber attacks, which can be launched by any sophisticated computer user located anywhere in the world, let alone by a network of terrorist organizations or a hostile power.

Yesterday's tragedies open a new era for our security infrastructure and for our critical infrastructure here at home. Therefore, we must now have an expanded notion of precisely what is important to our national security, and that more expanded notion must encompass much of our critical infrastructure. Thus, we must be prepared to defend ourselves against threats from foreign armies, but also to defend ourselves against threats from sophisticated opponents who will use both conventional and cyber weapons to destroy or disrupt sectors critical to our Nation's functioning. And, they will attack, as they did yesterday, here at home.

Yesterday's attacks demonstrate how an organized, coordinated effort can be devastating to our Nation. But make no mistake about it. Those attacks were aimed at destroying buildings, killing people, and breaking our confidence in the same way future attacks can and probably will be aimed at paralyzing our financial markets, our utilities, our transportation systems, and other core aspects of our critical infrastructure that are dependent on computer networks.

Today, individuals or terrorists or nations with no chance of success against America on the battlefield can pose just as significant a threat to our society from the isolation of their homes or offices or terrorist camps.

The nature of our critical infrastructure has changed that much in the information age. And while it has clearly enriched our lives, it has simultaneously left us much more dependent and more vulnerable to attacks by insidious forces.

So examining the vulnerability of our critical infrastructure is the focus of this hearing, but it is not an issue new to this Committee. Two Congresses ago, we held a series of hearings on computer security issues, and last Congress, Senator Thompson and I authored and the Congress enacted a law aimed at enhancing the government's computer security. This year, Senator Bennett particularly has urged us to launch this series of hearings that we begin today on the vulnerability of our critical infrastructure. His very successful leadership of our government's response to the Y2K challenge aroused his concern on this subject and makes him a valuable partner in this effort.

In the resolution that is currently before the Senate, there is some appropriately strong language used, and it refers to a war against terrorism: "Ask our allies to continue to stand with the United States in the war against international terrorism." The resolution commits us to support increased resources in the war to eradicate terrorism.

I think the important thing to say as we begin these hearings today is that if we are serious about commencing a war against terrorism, which the acts of war committed against us yesterday certainly justify, we have to understand that it is going to be a different kind of war. It is not going to be a matter of a single retaliation against a single terrorist opponent. It will be a much longer, sustained, and comprehensive conflict in which we will need to be more aggressive internationally to root out terrorists and stop them before they strike at us, to demand that our allies join us in pressuring and insisting countries around the world that harbor terrorists to decide whether they want to be our allies or the allies of our enemies, and to raise our defenses here at home against the kinds of insidious acts that we suffered from yesterday.

This means that we are going to have to consider, I think, some of the ideas that have been discussed previously in this Committee, and others, that came out most recently from the commission headed by our former colleagues Warren Rudman and Gary Hart as to whether we need an agency or even a department which is committed to homeland defense—a subject we have not had to worry about before, thinking that the oceans at least protected us from attack. But in the rising and escalating series of terrorist acts committed against us here at home, from the World Trade Tower attack 8 years ago, to Oklahoma City, and now culminating in the outrage yesterday, I think we have to begin to think about defending our homeland, just as we have thought and acted to defend our interests, our people, and our principles previously around the world.

I look forward to having this Committee, on a bipartisan basis, consider these questions and, as appropriate, make recommendations to our colleagues here in Congress.

Senator Thompson.

OPENING STATEMENT OF SENATOR THOMPSON

Senator THOMPSON. Thank you, Mr. Chairman. We commonly thank the Chairman for holding hearings, whether we mean it or not, but I think today we all mean it when we say that. It is very appropriate that we continue on with our work here and not be cowed into disrupting the work of the American people. I think that is what we expect, and this is certainly a very timely hearing.

I think we are reminded that, contrary to perhaps our thinking since the end of the Cold War, that the world is in many respects a more dangerous place than ever before, instead of less dangerous. The Soviet Union threat has been replaced now by several other threats that are more insidious and dangerous in many respects than the ones that we used to face. We face them from many different sources. We face them from rogue nations. We face them from terrorists. We may face them from combinations of both.

While much speculation now is on Bin Laden as far as yesterday's activities are concerned, it seems quite clear that he does not have access to 767's on a regular basis in order to train pilots to the extent to which those pilots were clearly trained. So the question becomes whether or not it is a combination of terrorist and state-sponsored activity.

We face many different kinds of threats. I think we, unfortunately, spend too much time in Congress debating on which threat is more likely, even though you would think we would be a little more humble about our predictions in light of yesterday's activities, which no one expected the precise nature of that particular attack. But we know we face threats from missiles which could make the casualty numbers of yesterday look small in comparison. We face them from suitcase bombs, conventional attacks, and, of course, cyber attacks, which is the primary subject of today's consideration.

You mentioned the Hart-Rudman report, and I think it is especially apt. I took another look today. I had read it in times past. It is one of several reports that we have had over the last few years, at least going back to 1998. We have to be told so many different times and so many different ways in this country that something is important before we pay adequate attention to it, and we have report on report now, Governor Gilmore's report, others, numerous witnesses testifying before numerous committees about the nature of this threat.

But going back as late as January 31 of this year, when they submitted their last volume, Hart-Rudman said, "One of this Commission's most important conclusions in its Phase 1 report was that attacks against American citizens on American soil, possibly causing heavy casualties, are likely over the next quarter century. This is because both the technical means for such attacks and the array of actors who might use such means are proliferating, despite the best efforts of American diplomacy."

It further says, "This Commission believes that the security of the American homeland from the threats of the new century should be the primary national security mission of the U.S. Government." It says, "However, the United States is very poorly organized to design and implement any comprehensive strategy to protect the homeland." It says, "The U.S. Government has not adopted homeland security as a primary national security mission. Its structures and strategy are fragmented and inadequate."

And it points out that, "These attacks may involve weapons of mass destruction, weapons of mass disruption. As porous as U.S. physical borders are in an age of burgeoning trade and travel, its cyber borders are even more porous." And, of course, the cyber threat is one of the major threats that we are facing here today and something that this Committee has dealt with over the last several years.

So I agree with you, Mr. Chairman, that we have to change our way of looking at things. We have got to get more serious about the threats to our country. For me, I think it starts with our military budget. It is hard for me to believe that we are still apparently debating irrelevancies like lock boxes and things of that nature that some people would prioritize over our national defense. We are

going to have an appropriations budget, and we will have an appropriation bills and an opportunity to address that in the near future.

There have been other instances of democracies who have taken their peace divided and ignored the clear threats around them and have thought that technology could bail them out in case of real problems and have ignored the misbehavior of nations around them that are weaker at the time that it starts. But the nations, the democracies have a tendency to turn inward and want to reduce their military budgets and think that the last war was the last war. All those mistakes England made after World War I, we must not go down that same road, and that has to do with military budget, including intelligence activities, including attention to our infrastructure, which is part of this exercise and our hearings today.

I think our witnesses will indicate that we haven't gotten very far in terms of the Presidential directive in 1998 that came down to try to organize this. You and I joined together, got a bill passed that we felt would improve our computer security. Perhaps we are set on the right path. I am not sure. But the word that I am getting from the progress we have made over the last few years is not good.

If there is something good to come out of yesterday, perhaps it will be a heightened awareness that we must do better. So, again, thank you for calling these hearings today.

Chairman LIEBERMAN. Thank you, Senator Thompson.

Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you, Mr. Chairman.

Yesterday, this hearing was one of our standard oversight hearings to assess how the government was securing critical infrastructure, including a Presidential directive that set as a goal the protection of the Nation's critical infrastructure, both physical and cyber, by the year 2000. With yesterday's events, terrorism has again demonstrated its evil face and has demonstrated this time the scope of its ability to inflict devastating damage on the United States. We, as a people, will do everything in our power to demonstrate our ability to deter such acts and to respond swiftly and severely when they occur.

Yesterday, terrorism destroyed the World Trade Center and the thousands of lives working in those buildings. It did serious damage to the Pentagon and caused a significant loss of life there. It destroyed the lives of 266 passengers and crew on four commercial airplanes. We run the risk that terrorism will disrupt our vital computer services which control our airspace, our information systems, our product distribution systems, our energy products, our entire economy.

The witnesses today will report on some of the efforts that we are making to protect our infrastructure where we have made some progress and where we have fallen short. But this hearing just puts words on what we already know because of what we witnessed as a country yesterday.

It is also important, it seems to me, to note that we also witnessed yesterday a determined and a unified response in our people to the horror and a determination to track down and to root out

and to relentlessly pursue terrorists, states that support them, and states that harbor them.

The terrorists are the common enemy of the civilized world. Our institutions are strong and they will prevail, but in the meantime, I think we should note that our unity here is absolutely palpable.

Each one of us, each of our committees, has a special responsibility, and I know that we are united and determined to carry out that responsibility, as this Committee has in the past and will today, and will in the future under the leadership of Senator Lieberman, and before him, Senator Thompson.

I hope you will excuse me, Mr. Chairman. I am on my way to a meeting of members of another committee, the Intelligence Committee, that is reviewing the intelligence budget and whether or not there should be recommended additions to that, perhaps in a supplemental appropriation, to try to see if we can't deter and address the places where we are not strong enough, particularly in the area of human intelligence.

Thank you.

Chairman LIEBERMAN. Thanks, Senator Levin. Senator Bennett.

Senator BENNETT. Senator Bunning came first.

Senator BUNNING. That is all right. Go right ahead.

OPENING STATEMENT OF SENATOR BENNETT

Senator BENNETT. Thank you, Mr. Chairman.

Like Senator Thompson, I appreciate your going forward with the hearing, and I appreciate your going forward with the issue. When I came on the Committee in this Congress, Senator Thompson and I had conversations about this, and I was very pleased with his enthusiasm and support for it. And now, with the change of leadership in the Committee, that enthusiasm and support has not diminished at all, and we are very grateful to you for that.

A lot of references have been made to yesterday, aside from the obvious concern about lives and the devastation. If I might be a little bit analytical for a moment, this was an attack on infrastructure, it was not an attack on the military infrastructure, even though the Pentagon, of course, was part of it.

But at the World Trade Center, as a result of that attack, the perpetrators succeeded in shutting down the air traffic control system, which is a vital part of our Nation's communication pattern. Mail goes by air. People that are necessary for conferences and communication go by air. And that is an infrastructure issue, separate and apart from the military, that was shut down as a result of this attack.

The financial markets, Wall Street couldn't open. The physical devastation on Wall Street made it impossible for trading to go on, and Americans were out of the financial world. Trading occurred only in Europe and in other markets, but not in ours.

And then just think for a moment about the long-term infrastructure devastation of the loss of all of the records that were there in the World Trade Center: Law firms that lost copies of wills, contracts, other things that would normally be available that have to be reconstructed now in one way or another in order for business to go ahead; transactions in progress that now have to be reconstructed from the beginning. Quite aside from the loss of life, which

is our first and primary concern, and always must be, the economic devastation that came out of that attack on infrastructure is going to take billions of dollars and months if not years to repair.

So it is a horrific reminder of the fact that outside of government is where most of the economic and social activity in this country goes on, and the traditional kinds of attacks against government are going to be less and less attractive to somebody who wishes us ill than attacks on infrastructure, whether it is by computer or by airplanes that have been hijacked, or whatever it might be.

So the question arises with this Committee's jurisdiction how well organized are we to deal as a government with this new kind of threat. I have taken the liberty, Mr. Chairman, of preparing a chart,[1] and it is put up there, and I will be happy to give you and Senator Thompson a copy, and Senator Bunning. Here is another version of it that shows how the Executive Branch is currently organized to deal with this particular challenge. It is not quite as helter-skelter as it looks. There is some degree of order in it, and it comes as the first attempt by the Clinton Administration with Presidential Decision Directive 63 (PDD 63) to get their arms around this. And I applaud that effort on behalf of President Clinton and the others, but it clearly needs some more rationalization. And if may be so bold, as Hart-Rudman recognized, the Congress itself needs some reorganization to address this problem and bring some kind of coordination and focus to it.

If I could conclude, Mr. Chairman, with this analogy: In 1986, when you were here but I was not, Goldwater-Nichols reformed the Defense Department from these kinds of charts of competing services and redundant missions. Without Goldwater-Nichols, I think every military historian would agree we could not have mounted Desert Shield and then Desert Storm. If we had gone into that military challenge with business as usual, we would have spent far more money, more time, more lives, and possibly not achieved anything like the result we achieved.

I like to think of this effort as a modern Goldwater-Nichols kind of effort, to say let us reorganize the government around the new realities that we face in protecting our critical infrastructure, reorganize the Executive Branch, and reorganize the Congress to recognize and deal with this challenge so that when there is a challenge in the future, some future Senator sitting here can say without Lieberman-Thompson, or whatever the names are that go on it, we would not have survived that. And I would hope that this hearing would be part of the process to bring a Goldwater-Nichols type solution to this enormously difficult problem. Thank you.

Chairman LIEBERMAN. Thank you very much, Senator Bennett.

Senator Dayton.

OPENING STATEMENT OF SENATOR DAYTON

Senator DAYTON. Well, thank you, Mr. Chairman. I just wanted to commend you and the Ranking Member and others for your foresightedness in scheduling this hearing. It was almost prophetic,

[1] The chart entitled "Critical Infrastructure Protection Organization September 2000," submitted by Senator Bennett appears in the Appendix on page 87.

given what occurred yesterday, and I look forward to hearing the expert testimony. Thank you.

Chairman LIEBERMAN. Thank you. Senator Bunning.

OPENING STATEMENT OF SENATOR BUNNING

Senator BUNNING. Thank you, Mr. Chairman, and thank you for holding this hearing after the horrendous day we had yesterday.

Before I begin, I would like to express my deepest sympathy and condolences to the families and friends of all those injured or killed in yesterday's attacks. This is a very difficult time for the Nation, and we must all work together to pull through it.

Protecting our critical infrastructure is of the utmost importance, and I hope this hearing today will shed some light on ways that we can improve the security of our Nation's computer system and infrastructure.

Our critical infrastructure impacts almost every aspect of our lives, from our Nation's security to our drinking water, to our financial transactions and communication services. Over the years, we have become more and more reliant on computer technology and the information that passes over it. Key industries in the Federal, State, and local governments have a responsibility to do everything possible to protect their information from hackers. Not only are they under attack from teenagers who are out for a joyride on the Internet, but individuals working for foreign governments, spies, and criminals can sit at a computer in another country and try to hack their way into some of our most important and sensitive information. Also, as new technology comes into use, it brings with it new challenges for businesses and the government in protecting private information.

I want to thank our witnesses for being here today and look forward to hearing the testimony that they are about to share with us about protecting our critical infrastructure.

Thank you very much.

Chairman LIEBERMAN. Thank you very much, Senator Bunning.

We will turn now to the witnesses. We are going to hear today from Roberta Gross, who is NASA's Inspector General and will tell us about a review of the implementation of the Federal Government's computer security policy conducted by the President's Council on Integrity and Efficiency. This was a review of the PDD 63, a Presidential Decision Directive. And we are also going to hear from Joel Willemssen of the GAO, who will discuss the government's efforts to work with the private sector to detect and respond to cyber attacks on critical infrastructure.

We had intended to have other witnesses here today who have been unable to be here, either because of the aviation shutdown or because they have been called away to respond to yesterday's attacks, and we hope on another occasion that we might have them here before us. But for now, we thank the two of you for being here, and, Ms. Gross, we now ask for your testimony.

TESTIMONY OF HON. ROBERTA L. GROSS,[1] INSPECTOR GENERAL, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Ms. GROSS. Thank you. I appreciate the opportunity to testify before this Committee. It is very difficult to stop a terrorist bent on suicide. We all heard this yesterday during broadcasts, both local and national. Did we ever imagine that we would have a suicide attempt at the magnitude that we experienced? Did we ever imagine that terrorists would use our own domestic airplanes as a weapon against our financial and military institutions? Probably not, or not in America. But we, like all nations, are a Nation at risk, and that is why this hearing is an important hearing.

After the Murrah Federal Building bombing in Oklahoma City, the government decided that it needed to have a strategy to address these new types of threats and vulnerabilities. The threats are from cyber terrorism which, because of the network's interconnectivity, might dislocate our financial, our electrical, our military, our communications, our government services, how we do business, how we live.

Clearly, we now know the threats can also be physical. We knew that before because not only was it physical threats like yesterday, we had physical threats in Oklahoma City and the Lockerbie airplane crash.

Whatever the form of threats, this Nation must have an effective national response so that our government, our economy, and our basic lives can go on. That was the purpose of the last administration proposing the Presidential Decision Directive 63. PDD 63 was a requirement, "for every department and agency of the Federal Government to be responsible for protecting its own critical infrastructure." And then other agencies—I think this chart (Senator Bennett's) is a remarkable mapping of some of the responsibilities of the coordination of agencies' responsibilities . . . had specific tasks to coordinate with the private sector to ensure continuity of communications, the Commerce Department; banking, the Treasury Department; aviation and highways, Transportation Department; emergency law enforcement, the FBI and Justice Department; emergency fire service continuity of government, FEMA; and so on and so on.

There are also different entities within the Federal Government to oversee this process, a Critical Infrastructure Assurance Office that was out of the Commerce Department; the National Security Agency; and OMB. (Again, I think this is a remarkable chart that really is the media becomes the message.)

I am proud of the collective efforts of the Inspectors General for their role in helping their agencies as well as the government, as a whole, build a strong protection of the infrastructure. The NASA OIG on behalf of the PCIE and ECIE—and those are the collective organizations by which the Inspectors General meet to look at trans-governmental issues—continue to look at agencies' implementation of PDD 63. And let me just briefly summarize that it is a four-part review.

---

[1] The prepared statement of Ms. Gross appears in the Appendix on page 33.

The first part is complete. We looked at whether agencies had adequate critical cyber plans, and this effort dovetails the current effort of the IGs and their agencies under the Government Information Security Reform Act, GISRA, which this Committee played a very important role. In fact, I was one of the witnesses testifying in favor of the act when you proposed its predecessor, S. 1993. We (the IGs) have all submitted our agency and IG evaluations on September 10, and there will be an effort by OMB to evaluate these reports. So we thank this Committee's effort on this legislation. I think the law gave a focus that was needed by both the agencies and Inspectors General that were not looking at this high-risk area.

GISRA, as you know, the Government Information Security Reform Act, reviews the management, implementation, and evaluation of IT security. GISRA really does dovetail what we were looking at with the PDD 63. We have a current and very timely effort ongoing now with the Inspectors General on the critical infrastructures, the identification, and the plans on the physical planning and implementation. We are getting preliminary results in, and we will have Phases III and IV—the agencies are not only supposed to have plans, they are supposed to implement the plans, because plans collect dust. And so Phases III and IV for the Inspectors General will involve making sure that the agency's plans are adequate and that they are then implemented.

So what did we find? We did find some good starts, but it is an understatement to say more progress is needed. We found in part that there is a misunderstanding as to the applicability of PDD 63. Some agencies just didn't start identifying their minimum essential infrastructure because they didn't know the directive applied to them, despite reading the directive that said "every and each." And part of that was because of the confusion as to who was in charge of implementing PDD 63. One of the major players had indicated if the agency was not listed in PDD 63 specifically as having a part, it didn't have a part, even though every agency is supposed to carry on its function and should, as an agency, identify what it needs to do to carry on its function in an essential manner.

What else did we find? We found that even those agencies that did have plans didn't necessarily identify all their mission-essential structures. They had confusing definitions. They had confusing performance plans. And so that made it very difficult.

The current administration is going to issue further guidance through an Executive Order on protecting the infrastructure, and I am sure this body, as well as all of the Senate and House oversight bodies, will be devoting attention to what else needs to be done to make sure our critical infrastructures are being protected.

I do want to say that I was happy to hear Senator Levin say that they are talking about the need for collection of information and human intelligence. I think that the people involved in security of our critical infrastructure believe that is a true need. I think one of the things I also want to point out—and I am sure that you have had hearings on this before—is that the laws to detect cyber criminals and to prosecute them are inadequate. In particular, there is not an anti-trespassing statute, and not having that statute only protects people who want to do ill against the cyber critical infra-

structures. You can have criminals come in ports that are not used for normal communication, and the laws do not allow law enforcement to ably protect these systems.

So, in sum, important steps have been taken and important steps continue to need to be taken to minimize attacks like yesterday, to avoid unknown terrorist attacks, whether cyber or physical. The IGs collectively and individually will be playing a role to help the Congress, their agencies, and OMB, get this Nation to a point where we are protecting all of our safety.

Thank you very much.

Chairman LIEBERMAN. Thank you for that statement. I look forward to asking you some questions.

Mr. Willemssen, thanks for being here.

TESTIMONY OF JOEL E. WILLEMSSEN,[1] MANAGING DIRECTOR, INFORMATION TECHNOLOGY ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Senators. In view of yesterday's tragic events, today's hearing I think reflects the critical importance of protecting our infrastructures. As requested, I am going to very briefly summarize our statement on efforts to protect Federal agency information systems and then, more broadly speaking, our Nation's critical computer-dependent infrastructures.

Overall, GAO's work continues to show that Federal agencies have serious and widespread computer security weaknesses. These weaknesses present substantial risks to Federal operations, assets, and confidentiality. Because virtually all Federal operations are supported by automated systems and electronic data, the risks are very high and the breadth of the potential impact is very wide. The risks cover areas as diverse as taxpayer records, law enforcement, national defense, and a wide range of benefit programs.

While a number of factors have contributed to weak information security at Federal agencies, we believe the key underlying problem is ineffective program management. Computer security legislation you introduced and which was enacted last year can go a long way to addressing this underlying problem. The legislation requires that both agency management and Inspectors General annually evaluate information security programs. OMB is due to receive the first reports from them this week. This new annual evaluation and reporting process is an important mechanism, previously missing, to holding agencies accountable for the effectiveness of their security programs.

Beyond the risks with Federal agency systems, the Federal Government has begun to address the threat of attacks on our Nation's computer-dependent critical infrastructures, such as electric power and telecommunications. The Presidential Decision Directive, previously noted as PDD 63, outlined a government-wide strategy to address this. A key element of that strategy was establishing the FBI's National Infrastructure Protection Center, or NIPC, as a focal point for gathering information on threats and facilitating the Federal Government's response to computer-based incidents.

---

[1] The prepared statement of Mr. Willemssen appears in the Appendix on page 43.

As we reported earlier this year, the NIPC has initiated various efforts to carry out this responsibility. However, we also found that the analytical and information-sharing capabilities that were intended had not yet been achieved. We, therefore, made numerous recommendations to the Assistant to the President for National Security Affairs and the Attorney General. These recommendations focused on more fully defining the role and responsibilities of the NIPC, especially in view of the many other organizations involved in critical infrastructure protection. Also, our recommendations focused on developing plans for establishing analysis and warning capabilities and formalizing information-sharing relationships with private sector and Federal agencies.

In commenting on our report, the administration said that it would consider these recommendations as it reviewed how critical infrastructure protection functions should be organized.

That concludes a summary of my statement, and I would be pleased to address any questions you may have. Thank you.

Chairman LIEBERMAN. Thank you both. I will begin. We are going to do 6-minute rounds, and we will keep going until Members have asked as many questions as they want.

Let me approach this through the Presidential Decision Directive 63, whose issuance was, I take it from what you have said, initiated or motivated by the terrorist attack at Oklahoma City, the Federal building.

Ms. GROSS. Yes.

Chairman LIEBERMAN. So we have a real-life event, a tragic event, a kind of precursor to what happened yesterday. And then comes a study, the Presidential Directive. Am I correct? And, incidentally, the directive covers both physical infrastructure in the normal, traditional way in which we know it, and cyber infrastructure in the new sense.

I take it from the consensus of the IGs—and I will ask GAO as well—that your judgment today is that the directive has been inadequately implemented, and in that sense, our critical infrastructure remains vulnerable.

Ms. GROSS. That is correct. I would have to agree with one of the Senators—and I think it may have been Senator Levin—that the United States is a strong, proud country, and when an emergency happens—as opposed to when an IG or GAO does a review . . . and we can find a lot of internal control problems . . . when an emergency happens like we had yesterday, there is a rallying in a way that, unfortunately, normally doesn't occur. So, in many ways, I think that the agencies recently were focusing hard on cooperating and coordinating.

But I think one of the failures under PDD 63-designated agencies and at each agency level, is what is the plan? What is the plan for the unknowns? And who is in charge, and how will that happen? I think that one of the things we were surprised at is for cyber, having gone through the year Y2K, is why didn't agencies have plans in effect for minimum essential infrastructure when, in fact, agencies could piggyback on their Y2K because they were supposed to be identifying key systems—they couldn't identify every system for Y2K compliance. Agencies would identify critical systems.

And if I even just look at the summary of the IG PDD 63 review comments from the different agencies, some of them said, "no, vulnerability assessment work is in progress; no, insufficient management attention to this level of detail"; "no, maybe some vulnerability assessments but no remediation plan because no funding"; "no, cause is lack of control over the various agencies"; "not performed because of other IT priorities."

The answers went on and on and on. It is hard to believe minimum essential critical infrastructure is not a priority.

Chairman LIEBERMAN. That is your conclusion, that it still remains that way?

Ms. GROSS. Yes. We are finding the same thing in the PDD 63 physical review. We are getting reports in from Inspectors General. We have 8 out of 16 that are going to be participating in this phase, and out of the 8, we have the same problems—plans not done, mission-essential infrastructures not identified, interdependencies not identified.

Chairman LIEBERMAN. What is happening? Why is this happening? Are people not taking it seriously, or were they not taking it seriously? Or was it not made a priority by the leadership of the respective agencies?

Ms. GROSS. Yes, yes, and yes. I think that what happens is everybody gets involved in programs. You see it at NASA. You see it at probably every agency that GAO has looked at. We want to get to Mars. We want to get the Space Station up. And what happens—and budgets go down, budgets get flattened, civil servants get flattened. And so people get focused on mission, and they forget about the infrastructure that supports the mission.

Low priorities become security, including IT security, oftentimes oversight functions like contracting oversight. Those are the kinds of things that look dispensable when you want to get to the moon, you want to get to Mars, and missions like that.

And so what happens is we forget the history of the Oklahoma bombing. We forget Lockerbie. Nobody is going to forget yesterday, I think it was so massive. But what happens is that then everybody stops putting attention on and a focus on these issues, and these are the issues where, if you look agency by agency, there is not the funding and there is not the support.

Chairman LIEBERMAN. It is a very important point. I mentioned before that we are beginning to use again the terminology of "a war against terrorism," and it is not bad terminology if we understand it is a different kind of war. And part of it is going to be fought here at home in areas that are not normally involved in defense. But they are involved in helping the government and the private sector protect the critical infrastructure.

Ms. GROSS. That was a financially cheap attack for the terrorists. I mean, if you think about yesterday's attack——

Chairman LIEBERMAN. Yesterday, with enormous consequences.

Ms. GROSS. With enormous consequences.

Chairman LIEBERMAN. And very costly, as my colleagues have said.

Ms. GROSS. And so that we need to focus on—it is not cheap for the cost to human life and re-creating it. And so we are having to

put some attentions where the kinds of wars are going to be different, and they are going to be cheap for the other sides.

Chairman LIEBERMAN. Right.

Ms. GROSS. And I put it as "sides."

Chairman LIEBERMAN. Yes. Mr. Willemssen, let me ask you, you mentioned the probability that the new administration will be issuing a new Executive Order on this subject. Based on your work, what do you think are the most important issues that should be addressed? And I suppose that is another way of asking what are the major weaknesses in our current approach to infrastructure protection.

Mr. WILLEMSSEN. Among the most critical issues is clearly identifying roles and responsibilities of the players. I think it is especially important for everyone to know who is exactly in charge overall and then within particular sectors. When players who are to some degree involved in critical infrastructure protection see an organizational maze such as that, (points to chart) it becomes very difficult to understand and to coordinate all the activities associated with infrastructure protection. So that is one especially critical element.

The second critical element is being in a position strategically to understand the threat and warning capability. That is not at this point from a cyber perspective where it needs to be.

Chairman LIEBERMAN. Say a little more so I understand what you mean.

Mr. WILLEMSSEN. Well, let me contrast individual incidents which occur and we are positioned to understand, OK, this incident happened.

Chairman LIEBERMAN. So give me an example.

Mr. WILLEMSSEN. An example would be the most recent Code Red virus.

Chairman LIEBERMAN. OK.

Mr. WILLEMSSEN. By stepping back and starting with each of the key sectors that have been defined, the eight key ones, first understanding what is the extent of the threat here, where do we think we could possibly get hit, where are our risk points. Second, what is the probability of those threats materializing? And if they do, what kind of severity, what will be the adverse impact on us? Taking all that into consideration, you then model a strategy to combat that.

In some cases, if the threat is huge but the impact is nil, you don't put a lot of effort into it. And, conversely, if you have got a high threat and a high impact, then we need to make sure that we are going to be protected.

Chairman LIEBERMAN. And thus far you haven't seen that kind of thinking.

Mr. WILLEMSSEN. Progress has been slow in that particular area.

Now, part of the challenge here in infrastructure protection is this is a public-private partnership, and so the Federal Government needs to work closely with the private sector in moving forward and achieving the goal of having a full operational capability by 2003. One of the key impediments to getting there is that the private sector, for good reasons, does not always want to share information related to threats, what the risks may be, what kind of

incidents have occurred in the past, all the kind of information that can give us a sense of where we stand strategically and where our risks are.

Chairman LIEBERMAN. It is a very important point. My time is up, and if my colleagues don't get back to it, I will. I thank you.

Senator Thompson.

Senator THOMPSON. Thank you very much, Mr. Chairman.

I think, Ms. Gross, you are absolutely correct about the different nature of the threat we face today and that the threats may be cheap for the perpetrator and expensive for us to deal with. However, I hope that we begin to spend less time on trying to evaluate the probabilities in terms of these threats and what we are most likely to be attacked by, because we can't predict these things, anyway, and realize that as the world's number one target, and likely to remain so, we have to guard against all of these threats. And it is a matter of our own priorities.

You point out some familiar themes when addressing this problem. One is management. So many of the problems that this Committee sees get back to the overall management issue. That has to do with priorities and the squeaky wheel and so forth. Unfortunately, it takes an event like yesterday sometimes to really get our attention.

We have a new administration, and every administration that comes into office now is taking longer and longer and longer to get its team together. So you have a National Security Adviser who, from day one, is faced with the most serious national security problems imaginable. And we expect her to kind of supervise this whole thing and these minute details that we are talking about here, totally unrealistic. So, it is multifaceted in terms of dealing with it.

I notice, Mr. Willemssen, one of the things that you pointed out is a lack of methodology, even to analyze the threats. How do we develop a methodology?

Mr. WILLEMSSEN. One approach that we would suggest is getting the top experts in the field who have experience in this area reaching agreement on the methodology and then essentially using that as an approved model to go forward.

Senator THOMPSON. Why should that be so difficult? Why should that take 3 years and we still do not have one?

Mr. WILLEMSSEN. I wouldn't minimize the chart that Senator Bennett's placed up there——

Senator THOMPSON. Senator Bennett's chart?

Mr. WILLEMSSEN [continuing]. As a key factor in that, and, second, the other issue I mentioned in this is a public-private partnership. This is not something that the Federal Government can simply mandate is going to be done.

Senator THOMPSON. Yes, and our critical infrastructure is in private hands for the most part, and it requires cooperation in order to address it. And yet you are asking private industry to perhaps reveal some of their most sensitive information, saying, "We are from the government, we are here to help you." And I don't see them doing that willingly under any circumstances. How do we break through that fear and skepticism on the part of private industry?

Mr. WILLEMSSEN. Again, Senator Bennett is very familiar with this, but there were some of those same concerns as we went through the Y2K situation, and there was legislation enacted to try to provide private entities some protection in the event that they were sharing information. And I think in retrospect that legislation turned out to be an outstanding piece of legislation.

Senator THOMPSON. That is a good analogy.

Senator BENNETT. Have I got a bill for you. [Laughter.]

Senator THOMPSON. You also mentioned in your report leadership vacancies. I alluded to how difficult it is becoming to get an administration together. We are talking about over a year now—a fourth of his term is over—before a President has his team together. I take it that is certainly—these are not high-profile positions, are they, that get a lot of attention and a lot of appreciation in normal times, I take it? Is that part of the problem?

Mr. WILLEMSSEN. I would say up until yesterday, you are correct, Senator.

Senator THOMPSON. Well, again, hopefully we once again identify the problem, and you certainly have done that. Both of you have done excellent work in this area. I was looking over the GAO reports done for the Governmental Affairs Committee just on information security alone, nine major reports that GAO has done on this very issue.

And lest we forget, what we are talking about, the CSIS did a study in 1998 and reminded us that, using the tools of information warfare, cyber terrorists can overload telephone lines with special software, disrupt the operations of air traffic control as well as shipping and railroad computers, scramble the software used by major financial institutions, hospitals, and other emergency services, alter by remote control the formulas for medication at pharmaceutical plants, change the pressure in gas pipelines to cause a valve failure, sabotage the New York Stock Exchange, not to mention military command and control.

Finally, you have spoken favorably toward Senator Lieberman's and my computer security law. It sunsets next September. Because we were in negotiations with the House, quite frankly, we had to accept a 2-year sunset. I hope that we can count on your support to get past that sunset. Senator Lieberman, that might be something we want to address right away.

Chairman LIEBERMAN. Good idea.

Mr. WILLEMSSEN. Yes, sir.

Senator THOMPSON. Thank you very much.

Chairman LIEBERMAN. Thank you. Senator Dayton.

Senator DAYTON. Thank you, Mr. Chairman. Again, I want to commend you and the Ranking Member and other Members of the Committee who, for some time—years, in fact—have been delving into these areas that we realized yesterday we cannot take so much of what we take for granted for granted. And I also certainly want to associate myself with the remarks of Senator Thompson regarding the unbelievable and unacceptable length of time it takes to fill an administration. I serve on the Armed Services Committee. I know Secretary Rumsfeld has opined on that matter to us, and if the events of yesterday had occurred 2 months or 4 months after the President took office, and as the Secretary said at the time, he

was literally in that suite of offices alone, it would have been even more overwhelming, I would suspect, than it must have been yesterday. So I think that would really be a very fitting subject for this Committee to address and really try to assure that no subsequent administration has to endure those kinds of delays.

Again, my experience over the last 8 months has been primarily on other committees, and in the Armed Services Committee, in both public and private meetings and briefings, no one portrayed a scenario that even approached what occurred yesterday in terms of the threats of terrorist attacks and the like. So, on the one hand, I don't want you to be unduly alarmist. On the other hand, I think maybe we need to be more alarmed than we are in these critical areas. And I wonder if either of you or both of you individually would paint for us a scenario of what a major, well-coordinated, highly sophisticated assault on these systems might look like for our country.

Ms. GROSS. I think we saw one yesterday.

Senator DAYTON. Well, yes, physical assault, and obviously, that involved others, but in terms of——

Ms. GROSS. You could have it from the computer by having massive denial of services, which hackers are able to do by taking tools of the Internet, so that you can have hackers who have terroristic motives using juveniles who think that this is fun but they don't know they are being used. You can also have it be for individuals who see it as an opportunity for economic espionage, and it is an opportunity to get either companies' information, and so that you can have a coordinated—you can have a mastermind by some terrorists who are using other entities who don't even know they are being used, so that you have viruses, Trojan horses, denial of services. You have tools being implanted in critical systems, non-sensitive systems, so that they will then be available for an attack later. Everybody thinks it is all over, we finish with the Red virus, we finish with the denial of services, yet they park their tools basically at NASA's systems, at EPA's systems, and at other systems, and they just wait then for another onslaught and nobody is looking. You have systems administrators who haven't been trained, who are having privileges for root access without training. You have multiple people who have root access that shouldn't have root access. You have common vulnerabilities. And so the cyber terrorists have the tools there waiting for the event to happen because we don't shut down no-cost, low-cost vulnerabilities. It is waiting to happen.

Senator DAYTON. Mr. Willemssen.

Mr. WILLEMSSEN. Yes, Senator, in addition to those kind of risks which can focus on disruption or stoppage of operations, which becomes especially critical when we are in a real-time command and control environment, there are also the kinds of risks that don't always attract as much attention, but they are still important, and that is the inappropriate disclosure of sensitive information.

For example, in work we did after the 2000 filing season at the Internal Revenue Service, we were able to penetrate their systems and browse data. We could have changed the data if we wanted to. There are also those kind of impacts in terms of the sensitivity of information, the disclosure of that information, and also the ability

to either change or modify or destroy that data. So there are those associated impacts in addition to the work disruptions, work stoppages.

Senator DAYTON. Maybe I didn't phrase my question eloquently enough, but I just would leave for our future consideration, I mean, what you both describe accurately are akin to what I heard in other settings as individual terrorists with a suitcase, a car, or whatever. What we saw yesterday was something that in its scale and its sophistication and coordination greatly exceeded at least anything I had heard described as a possible scenario, and as a result I think really overwhelmed our system because we in a sense hadn't imagined how dastardly the deeds could be. And I would hope that that is being done, and maybe akin to that—my time is almost over—how do we prevent the invasion of one system, one agency, or whatever, from being then the conduit to go to all others, especially as these systems reap the advantages of being more interconnected with one another?

Ms. GROSS. A layered approach, and they have got to be starting—I mean, you had to start yesterday, but you have got to certainly start now. If you don't have as one layer a bully pulpit from the administrator of each agency, from OMB—and I think GISRA will play an important part of it—a priority. Employees have to hear it at every meeting. Layering requires password controls, training, and software installed only for desired uses. That is for the Federal Government control. There is a whole side—again, when you talk about the public-private partnership, why are private industries allowed to rush to the market with vulnerabilities on the market? We are vulnerable. They know better than we do. We find out about these vulnerabilities. The hackers find out and put them on their web pages.

But you have manufacturers rushing to put their software out, and then agencies install the softwares on their systems which later require "patches." If you want to also talk about the public-private partnership, the private sector has got to be responsible because they are developing the software that we use, by and large. Both the Executive Branch as well as the Congress is asking more and more agencies to go use off-the-shelf software. I saw that even—I think it is NSA, or NRC, I can't remember which one—is going to use off-the-shelf software.

So if you want to talk about something that has to be paid attention to, this off-the-shelf software cannot be coming to the government and others with vulnerabilities. There have got to be some warranties.

Mr. WILLEMSSEN. Let me just add, Senator, the Inspector General has talked about the protection side of computer security, which is critically important, and we need to place a lot of resources on that. One caveat to always keep in mind is we can never provide absolute protection whenever we are communicating electronically. That is why the other two legs of what we refer to as a three-legged computer security stool are especially important, not only protection but detection and prosecution. Detection so that when somebody gets in immediately, and you take prompt action, and then prosecution, you have to go after the perpetrators.

Senator DAYTON. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Dayton. I appreciate your asking the witnesses to go forward and project how a cyber attack might occur against us, because obviously we hold a hearing like this to gauge how realistic these threats are so that we will never have to look back and say, gee, we never knew this was possible. And, of course, the other part of it is that ourselves, together with the Executive Branch and our IG friends and the GAO, will motivate some action to protect us from those threats.

Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman.

Mr. Willemssen, I didn't set you up as a straight man, but I do have a bill patterned after the Y2K bill to deal with the issue of disclosure between the government and the private sector in circumstances that we have never had before. Go back a decade, and there would never be any anticipation that we would need private industry to explain to government agencies what kind of attacks they are receiving and vice versa, sharing of information. And I think the Freedom of Information Act, which we amended with respect to Y2K and to which you referred, has got to be amended again in this circumstance. And you are nodding, but I will ask for the record the obvious question: Do you agree that we need something of that kind?

Mr. WILLEMSSEN. I agree that that would be a great motivator to enable increased sharing of information between the private and public sectors, which is absolutely critical.

Senator BENNETT. Now, you talk about the three-legged stool. When we have had hearings on this subject in the Joint Economic Committee, the witnesses have pointed out that part of our problem is that we need to think strategically rather than tactically. And tactically comes down basically to law enforcement and prosecution after the fact. Thinking strategically is asking the kinds of questions that have been asked here of what could happen and what do we need to put in place before the fact.

One of the criticisms I have of PDD 63—and I repeat once again, I applaud the Clinton Administration for the action that they took in moving in that direction. But we need to move more.

One of the criticisms I have of PDD 63 is that it puts the primary responsibility with the FBI and with people who have a law enforcement mentality. If you have a law enforcement mentality, you wait until a crime is committed, and then you go look for the bad guys, arrest them, and haul them to jail.

In this circumstance, we can't wait for the crime to be committed, and for that reason, I think the FBI and the Department of Justice is not the right place to have the primary domestic responsibility. I think we have to do the kinds of things which were hinted at in your testimony, almost a red team/blue team approach of let's take a red team into the Department of Commerce and see how easy it is to break in and see what kinds of chain reaction can be established.

Again, I have used this example where an IT supervisor in his company suddenly discovered that someone was in, and so he hacks back to find out who it is and finds himself at root level, which means he owns the system of a Canadian company. He calls the company on the telephone and says, I am at root level in your

computers, which means I can do all the things you were describing, Mr. Willemssen. I can change your passwords. I can steal your data. I can scramble the data so that you can give false instructions. I can do whatever I want. Are you aware that you are being used as a conduit to get into me? And the Canadians were unaware that their computers had been used in that fashion. They were very grateful for the phone call.

But the fact is that under existing law, the American could be sent to jail for having gotten into the Canadian computer to that degree. So a strategic analysis of what do we have to do to protect ourselves has to trump a law enforcement attitude that says, well, we don't care what you did to protect yourself, but under this law you broke the law.

Now, the Canadians obviously did not seek to prosecute. They were very grateful that this man helped them understand their own vulnerability.

Could you address that whole general question of what kinds of strategic moves you would recommend, red team/blue team approach or anything else, as to how we might build a strategic attitude and then we go to work on the chart? Once we have the attitude and the vision where we want to go, then we move the boxes around on the chart as to who does what?

Mr. WILLEMSSEN. Yes, I would like to address that. We found ourselves at GAO with a similar predicament a few years ago of trying to be in a position of convincing agencies that they really needed to do a better job of protecting their key assets. In response to that, we elected to develop our own internal capability to penetrate systems, our own white-hatted hackers, so to speak, that we have used over the last couple of years at selected agencies and continue to use.

This approach has been very effective at demonstrating that we can get in, we can see this data, we can change the data.

The most recent department where we did that was at several bureaus at the Department of Commerce where we got in. We had root access. We were able to view a lot of very sensitive data. And, again, consistent with what you mentioned, in most cases Department officials didn't know we were there.

Now, when you share that kind of information with senior management, it does tend to be an eye-opener. And so I would concur with your approach on the red team/blue team. It is a very effective approach for getting top management focused on the issue and for them to understand there are some real threats here.

Ms. GROSS. I think yes and no. I mean, I think your red team/blue team is a very important effort. NASA was one of the agencies that GAO had reviewed but didn't use their own intrusion resources. I think they used another Federal agency for NASA. They successfully got into a mission-critical or a very critical system at one of the centers that we always call the Center of Excellence for Intrusions, and that center still has problems. NASA, to its credit, has come a long ways in doing policies and procedures. It is also hiring its own penetration testers. As part of the Chief Financial Officer's audit is having a penetration testing going on.

You got to keep bucking up that attention. GAO is only so big. We were talking about the assets they have for doing this. None

of us have enough assets. I think you had a focus from the GISR Act that is going to expire, but this is the first time that OMB is going to get reports from every agency. The agencies are going to give their opinion, and the IGs are going to give their opinion. There is no hiding. The agency may say, hey, everything is great, Pollyanna. And the IGs may say everything is horrible. And maybe the truth is somewhere on one side or the other.

But OMB is going to have to grapple with every agency, each agency's IG is learning how to do IT oversight better. You don't want to let that heat go off. You don't want to rely on GAO. They will cover us again maybe in the next 5 years. And, OK, we will have a hearing, probably before this Committee or another committee, and you will get NASA's attention, and we will come up with more policies and procedures. And you know what? We are still going to have vulnerabilities.

It is hard to make it risk-free. That is not the problem. But it has to be a kind of attention where the government is saying, Hey, we really do care.

I read to you earlier what was coming on our review from the PDD 63 for agencies on their mission-essential infrastructures on their cyber plans: Lower priority, not enough money, didn't know it applied to us. They should have been able to just roll over the Y2K information.

So, I think it is not merely just red team/blue team. You are going to have to keep a focus. I think sustained government oversight is a real key tool.

Chairman LIEBERMAN. Thanks very much, Senator Bennett.

I was reminded by Mr. Willemssen's answer to one of your questions about how they got the attention of the agency. Unfortunately, the folks from @stake, Inc. could not be here today.[1] They are part of a group we had here some years ago, when they were with another organization called the Lopht, which was a kind of think tank. They got out of that business because they were able to hack their way into major corporate computer systems to inform the management of vulnerabilities, and than offer these companies help gratis. But the capacity to do damage here, as you both said—and your tests prove—is very real.

Senator Bunning.

Senator BUNNING. Thank you, Senator.

I would like to just ask Ms. Gross, are you telling this Committee that the agencies of the Federal Government have this important project at the bottom of the list?

Ms. GROSS. Well, they had—some of them had PDD 63, which was a Presidential decision——

Senator BUNNING. Yes, I understand that.

Ms. GROSS. We are——

Senator BUNNING. I am talking about generally now, of all of the agencies of the Federal Government that deal with critical information on computers.

Ms. GROSS. Oh, all, I wouldn't say all. I think it has been a real low priority for a number of years. When the GAO was doing its exit conference for NASA and they reported the absence of the lay-

[1] The prepared statement of @stake, Inc. appears in the Appendix on page 78.

ers of protection an agency's supposed to have, that is, policies, procedures, education, intrusion detection, your own penetration studies—components needed to have a security program. At the end of the conference, one of the managers turned to the GAO person and said, "Do you have any good news for us?" And they said, "Yes, the good news is at least you are one of the agencies that has an awareness you have a problem." When they go——

Senator BUNNING. That is the attitude?

Ms. GROSS. We had awareness, partially because we had been doing work and then they started doing some of their own work. But what the GAO was saying is that other agencies were denying they even had a problem.

Senator BUNNING. OK.

Ms. GROSS. I think people are becoming more sophisticated about the problem.

Senator BUNNING. Sometimes there are very simple remedies to some of these problems, and I would ask Mr. Willemssen, you mentioned weakness as a result of some agencies not even deleting accounts and passwords of people who are no longer employed or change passwords. Now, how hard is that?

Mr. WILLEMSSEN. It is not hard at all. It is a matter——

Senator BUNNING. We do it in our office, and our office happens to be connected to the Senate office, but we change passwords on a monthly or bimonthly basis and do a lot of other things.

You mean to tell me that when someone leaves NASA, for instance, that you don't delete the password or you don't delete entrance to that——

Ms. GROSS. Not always. We have audits that show that. Not always.

Senator BUNNING. That is unbelievable.

Ms. GROSS. It is. Those are low-cost, no-cost kinds of remedies. When we are talking about not enough money, why agencies can't do things, there is a lot of low-cost, no-cost solutions and fixing 90 percent of the vulnerabilities are low-cost, no-cost. It is a matter of attention, starting from the top. It is using the bully pulpit by each agency administrator and department head that IT security is what they expect from each program manager. CIO's need to tell their agency heads if they don't have an education program. For example, one of the things that upsets me about NASA's program, we haven't trained our systems administrators. They have a metric on evaluating the training for systems administrator. They are the front-line people that manage and have root access to your systems. They have metrics on the civil servants system administrators, which they are tracking, though most of our systems administrators are contractors. It was in the low percentages as to the number of people who received the training.

Now, part of that is because the training components had not been finished, and that is for various and sundry reasons. But part of it was they didn't even have the money or staff.

Senator BUNNING. Well, but if you have a systems administrator, they ought to know who and who doesn't work, and they could automatically delete access to the system when a person leaves.

Ms. GROSS. There has to be a communication between the systems administrator and the program people. Sometimes the system

administrators is just—it could be a scientist doing a program. I mean, the system administrator is not necessarily——

Senator BUNNING. I am talking about the people that are in charge of the computer system. You can call them whatever you want to call them.

Ms. GROSS. Should it be easy? Yes. Should there be an easy system? Yes.

Senator BUNNING. What about the kids that hack for fun, that are hired for, unfortunately, bad things? They could have assisted in getting access to these aircraft by making reservations, by doing whatever is done to get a hijacker onto an aircraft, not knowing what was going to happen. Why can't we get those people?

Ms. GROSS. That is a good question. I think the Justice Department is starting a program that needs to be a major education effort. The government needs to get into the high schools and into the junior highs.

In my written testimony is one of the cases where both international and national activity were involved. A hacker from Israel was mentoring juveniles who were breaking into DOT systems—excuse me, DOD, the Department of Defense systems. And they thought that this was just a lark on their part. They were not intending to——

Senator BUNNING. How good they were that they could do all this.

Ms. GROSS. Yes. We don't know the full intent of what the hacker from Israel was, but, nevertheless, these were juveniles who think they are just on a lark and being smart, who were being used by and mentored and cultivated by somebody else. Your question is an important question. It is an important education process for the government to get into the high schools, to get into the junior highs, because sometimes adults use juveniles. It is just like what happened in the war on drugs where you have a minimum mandatory sentences for drug couriers in the District of Columbia, which I am very familiar with as a DC resident and I used to be with the Office of the Corporation Counsel. As soon as the city had a minimum mandatory sentence for adults for drugs, drug addicts used juveniles because for juveniles it wouldn't be a real sentence, they wouldn't be criminals. They would remain in the juvenile system.

And so you will have people who will be motivated to use juveniles because nothing will happen to the juveniles. And they won't know they are even being used. Your question is a key one, and I think that needs to be grappled with.

Senator BUNNING. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Bunning. Thank you very much. I share your sense of outrage and disbelief, and hopefully we can generate some reactions here.

Did I see Senator Carper? If not, for the moment I will proceed with another round of questions.

I want to go to the private sector involvement here. Maybe first I would just ask this question by way of setting the scene, the landscape. We distinguish traditionally between physical and cyberspace infrastructure. But Senator Bunning's question regarding the suggestion that it is quite possible that the terrorists yesterday had to—in this case, it probably was a fairly simple action—penetrate

some or at least use computers to determine flight schedules and gain access to them. Is it fair to say that there has been a kind of melding in our time of both physical and cyberspace infrastructure that to get today at the physical infrastructure, whether we are talking about a power grid or financial services networks or transportation, that you really are probably going to end up, in whole or in part, also in cyberspace?

Ms. GROSS. I think that was the philosophy behind PDD 63, is that the whole interrelatedness of our infrastructures, the critical infrastructures, could be shut down through a cyber attack. How interrelated we are, from a physical attack is clear, who could get through yesterday to New York? Even communication through some of the networks got shut down because of what was happening. The world between the network systems and the physical systems are so interrelated. We have a very efficient world, and we can do lots of work, and our economy was so strong, in part, because we are such a networked economy. But because we are interrelated, we are also vulnerable.

Chairman LIEBERMAN. OK. So let's ask about the private sector now because, as we said before, a lot of what we are describing—we have been talking a lot about what the government has done with our systems, but a lot of what we are describing—utilities, transportation, financial services, the rest—are private.

Give us a very brief overview of what the Presidential Decision Directive 63 asks of the private sector. How is it performing? And what more should we ask of it? In other words, Mr. Willemssen has referred a few times to the public-private partnership here. Is there a genuine working partnership going on?

Ms. GROSS. I would say on the education level universities are working—but, a simple answer is no, there is not really a public-private/partnership. I think that Senator Bennett is correct. We are going to have to talk about legislation and what is it that we need to motivate this partnership.

Some of what happened yesterday is going a long ways to motivate a partnership because the most vulnerable group was certainly in many ways the private sector. And the private sector is absolutely depending on the public sector for its rescue, and that is FEMA, FBI, Justice, Energy, all these entities are coming to help the private sector. So that is going to help cooperation.

But I think you are going to have to find the motivations for partnership. They are working on these partnerships for education. Universities are talking about being centers of excellence for IT security or for IT. The government is talking about forgiving loans. IT is setting up centers of excellence. But the university community is more used to working with the government.

Again, I go back to an earlier remark, it is important, you have to make sure that companies are not allowed to put known vulnerabilities into the market. But in terms of sharing those vulnerabilities, you have to talk about what is going to create incentives. Some of those are going to be carrots and some of those are going to be sticks. And I don't think we know.

Chairman LIEBERMAN. Is it fair to say that a business may have some evidence that it has been attacked?

Ms. GROSS. Yes.

Chairman LIEBERMAN. And it is a very interesting and difficult question as to what is the point at which that business should feel a responsibility. Should we require by law that it report that to government? Because it may, of course, be the beginning of a more broad-scale attack on a critical infrastructure, a utility, an airline, a bank, the Federal Reserve—well, a bank. Let's stick with that. What is happening on that front now? I will get you in on this, Mr. Willemssen, too.

Ms. GROSS. Well, that is the $64,000 question in many ways. I mean, you have the FedCIRC—you have a number of entities where both the private and the public do participate in sharing information. It is not a law enforcement model. And I think that it bothers a number of entities to have that law enforcement model. I have a very strong cyber group, of which I am very proud, for criminal prosecutions. But, in part to deter bad acts, we do press releases, companies get publicity. Intrusions becomes known.

Chairman LIEBERMAN. And a lot of businesses don't want that to happen.

Ms. GROSS. Absolutely not.

Chairman LIEBERMAN. Even though they may be the first line of what is a larger attack on infrastructure.

Ms. GROSS. Yes. Some are becoming more courageous about it because they want to deter, they want to say we care and we will prosecute, so that they won't be held up. This is a very sensitive issue. If you say to people we are going to prosecute you, too, and you are not going to embarrass us, then you can't hold up people, for——

Chairman LIEBERMAN. Mr. Willemssen, why don't you talk a little bit on this subject? Because my sense is from what I have heard so far that the partnership, at least at the defensive level, between the public and public sectors is not—there is not much happening there.

Mr. WILLEMSSEN. It is mixed, and one way to look at it instructively is to take each sector individually because different sectors are at different stages of maturity in the extent to which they share information.

Chairman LIEBERMAN. Which are better and which are worse, would you say?

Mr. WILLEMSSEN. For example, when we ended our work on NIPC, the two areas which had established information-sharing and analysis centers were in the electricity area and in the financial services area. Those information-sharing and analysis centers, or ISACs, are your mechanisms for determining, OK, what are we all going to agree to share? What are the thresholds going to be when an attack occurs?

Chairman LIEBERMAN. And at what point, right?

Mr. WILLEMSSEN. And so these are very important mechanisms to try to pull together.

Now, some of the sectors are further ahead. For example, in the electricity area, you have the North American Electric Reliability Council. That already is a very good group of bringing everybody together. They like to partner. They have to partner. And so that has worked fairly successfully. Some of the other sectors are going to take some time.

I think from an oversight perspective, part of what you may want to look at is the particular lead agencies for those eight critical infrastructures and where are those lead agencies in helping to make sure that this gets done.

Chairman LIEBERMAN. In other words, the lead governmental agencies related to those sectors of our infrastructure.

Mr. WILLEMSSEN. Yes, sir.

Chairman LIEBERMAN. Which are largely private.

Mr. WILLEMSSEN. Yes, sir. And so if you were looking at Senator Bennett's chart, it would be on the right-hand side where it says "Lead agency," and then the ones going down, each of those has a lead for one of those eight critical infrastructures.

Chairman LIEBERMAN. OK. Thank you. That is a big part of the problem. Again, because they are not here, I will just take a moment—our two witnesses from @stake, Inc. who were going to be here—to read very briefly from the testimony they prepared for today. These are the former hackers who now are consultants at a digital security consulting and engineering firm: "It must be remembered that the mandate for these companies is to drive shareholder return, not to secure critical infrastructure. Today @stake, Inc.'s client base views security as a sunk cost, largely a product of information technology architecture and associated spending. Security is viewed as a cost borne to mitigate risks that may negatively impact the corporate mandate of generating shareholder return."

I am going to stop there. Senator Bennett, do you have a moment for me to call on Senator Carper?

Senator BENNETT. By all means.

Chairman LIEBERMAN. Senator Carper, welcome.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman. Thank you for calling this hearing, and I am pleased, in spite of the tragic events of yesterday that continue to unfold, that we are having this hearing. I think it is appropriate that we do express our thanks to our witnesses as well.

I apologize for arriving a bit late. I have a question that I would like to pose. When one arrives a bit late at a hearing, you don't know how many people have asked the same question so I would ask you to bear with me, if you would.

But I understand that there are some segments of our infrastructure which have done a better job than others in terms of providing the kind of security that we need in this day and age. There are others where there is some work to be done. And I would ask you just to again reiterate for us where you think some of the better work has been done and to mention several of the areas where we have our work still cut out for us.

Mr. WILLEMSSEN. I would say, Senator, that the banking and finance area is probably one of the more mature in its understanding of security risks and——

Senator CARPER. They have a lot at stake, so I could see that.

Mr. WILLEMSSEN [continuing]. Need for protection. I would say that is probably near the top of the list in terms of the evidence we have seen.

Senator CARPER. In terms of being particularly well prepared or better prepared than other segments?

Mr. WILLEMSSEN. Well, prepared from a protection perspective and a detection perspective, so that when they are penetrated—again, speaking very generally—they know it fairly quickly and take action.

Senator CARPER. What other segments of our private sector are maybe better prepared than others, and where are some that we might need to——

Mr. WILLEMSSEN. Again, I think the area of electric power has the advantage of a very strong organization, coordinating organization, North American Electric Reliability Council, which has served very well. I mean, obviously, all the members of that must work together, given the resources that we are talking about. So that is another one that you can point to, to some degree. Again, speaking generally.

Senator CARPER. What are a couple where we have our work cut out for us?

Mr. WILLEMSSEN. Well, I would say if you look at some of the other critical sectors, I would say a lot of work remains to be done in public health, especially as we continue to increasingly share medical data electronically. I think that is an area that will continue to require some attention.

I think the transportation area is hard to generalize. You kind of have to go by mode of transportation. But, again, that is an area that also will require more focus.

Senator CARPER. What advice do you have for this Committee and for the Senate?

Mr. WILLEMSSEN. The advice I would have is on a couple levels. First, we should think of our Federal agencies as setting a good example, I think, for the rest of the country, and that is why I continue to think that the legislation that was put in last year that is requiring these reports is an opportunity for the Senate to provide oversight and hold these agencies accountable for how well they are doing. And then, second, speaking more broadly on critical infrastructure protection, I think also the opportunity is there for you to provide oversight of those lead agencies for the critical infrastructures to inquire of them where they stand in reaching agreements with the private sector in making their ISACs, their information-sharing and analysis centers, a reality. And then to the extent that they aren't there yet, asking for some milestones and some tasks and then, again, holding them accountable to those.

Senator CARPER. Legislation has been introduced by our chairman and his immediate predecessor, Senator Thompson, that I would welcome your comments on, if you would.

Mr. WILLEMSSEN. Well, among the items in the legislation that we strongly support is the need for the Federal chief information officer setting the standards and the stage for the Federal Government on exactly who is in charge of information technology overall, including information security. I think the legislation has a number of other key elements that are especially important in the security area, in the area of e-government that we have got to start looking at providing services more from an electronic perspective, pursuant to existing law.

Ms. GROSS. If you look at the analogy with the Y2K, no agency head had any doubt that they were going to be held responsible if there was a failure. John Koskinen was a focal point appointed by the President as his adviser. He went both to the private sector and to the public sector. He went to agencies, he went to CIO's as well as agency IGs to find out if there were going to be problems. There were quarterly reports that went to OMB. There were reports by Congress.

There is nobody that had a doubt that this country was committed to making sure that when the new millennium happened we were not going to crash with all of our systems. And it didn't happen. There was a priority that was clear. It was the Nation's priority, from the Executive Branch to the Congress to program managers. And you need to have that kind of same priority, bully pulpit at all levels, and believability that there will be no—that nobody wants to have the failure and that everybody believes that it is an agency priority, it is a Congress priority, and it is an Executive Branch priority.

Senator CARPER. Thank you. One last question. Reflecting on what occurred in America yesterday and realizing that you may not be an expert in this area, what lessons do you think we have learned as far as transportation security goes?

Mr. WILLEMSSEN. A difficult question to address. I wish I knew more information about the effort yesterday.

I think one item that was mentioned earlier that is worth noting is that the demarcation between physical and cyber is becoming less clear. And so I think as the investigation proceeds on the events of yesterday, it will be worth noting, if there were any automated means which provided expedited tools to provide the perpetrators with an easier effort than otherwise would have been the case, I think that is something that should be noted as the investigations go forward.

Chairman LIEBERMAN. Do you mean to gain access to flight information? How did you mean anything that might have given the perpetrators——

Mr. WILLEMSSEN. Any tools that they could have used electronically that in the past may not have been there in terms of getting flight information, information on who is going to be on the flight, when it is taking off, when it is landing, any delays. To the extent that those are there today that they didn't used to be, and if it turns out those were major tools, I think that is worth noting.

Senator CARPER. I'm just thinking out loud now, but to the extent that there are people whom our intelligence officials know to be a possible threat to our country, and to the extent that they travel in our country, it would be helpful if we had the ability to know when they are moving, especially if they are moving in aircraft, obviously. That is something that we might want to be mindful of going forward, far more in the future than we have been in the past. Also, one of the things that struck me, aircraft as they fly, commercial and military and others, they carry equipment on the plane, transponders, which controllers can communicate with to find out the altitude of the aircraft, the direction of the aircraft, the speed of the aircraft, the identification of the aircraft, and pilots have the ability to trigger from the aircraft an automatic signal

that would indicate to anyone who is interrogating them from the ground whether there is a hijacking underway. One of the things we will be interested to find out is to what extent that technology could have been used by the pilots to alert someone else that there was an emergency.

We have heard of the several telephone calls, cell phone calls that were made from the aircraft, but I have not yet heard how that might have been used as a tool by the air crew to alert others that something was awry.

Again, Mr. Chairman, thank you for holding this hearing and for letting me join you.

Chairman LIEBERMAN. Thanks, Senator Carper. Those were very good questions and good points.

I would say to you that I spoke to David Walker, the Comptroller General, yesterday and Mr. Willemssen has focused on the matters to which he has testified and done so very ably. There are others at GAO who are focused on the security of air traffic systems and airport security, and I haven't had a chance to talk to Senator Thompson about this, but it might be that we would want soon, in the aftermath of yesterday, to call them in and see what their years of experience and reports, some of which were referenced in the newspapers this morning, tell us about what we can do after yesterday to protect ourselves in the future.

Mr. WILLEMSSEN. I would just add, Senator, I do have with me the Managing Director of GAO who is responsible for that area in the event questions on that come up at today's hearing.

Chairman LIEBERMAN. I appreciate that you did that. I think we will probably want to do that soon and focus on it separately at a hearing. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman.

Ms. Gross, again, we didn't coordinate in advance, but you are a great straight person.

Chairman LIEBERMAN. I am beginning to have doubts about this.

Senator BENNETT. Your references to Y2K and John Koskinen, I can't resist. As John was leaving government service, he and I talked, as we did every week through the whole Y2K experience. John and I talked every Wednesday afternoon, and I told him what we were doing here, and he told me what he was doing there. And we did our best to coordinate all of our efforts. He said, "I understand you are now interested in critical infrastructure protection, and you are going to push the Congress on that issue." And I said, "Yes, I am." And he said, "I think that is very important, and I congratulate you and applaud your efforts, and you will do it without me." [Laughter.]

Senator BENNETT. He said, "I am going to go back into the private sector. I am through with this business. And I wish you well, but I am not going to be involved."

There were some in the Clinton Administration that wanted him to be the CIO for the entire government, and he turned that down.

Ms. GROSS. He is working with the public sector still. You may know that he is working with the District of Columbia Government. He can't resist public work.

Senator BENNETT. He is an excellent public servant, and I thoroughly enjoyed my association with him.

But back to—as long as I am telling anecdotes—your reference to some people thinking of this in terms of sunk cost, and it is something we have to do, but we are not going to get any return on our investment. And that was exactly the attitude with Y2K. Everything we spent on Y2K is technically a waste of money because there will be no return on it at all; therefore, we need to spend as little as possible.

Looking back on it, we can say that was not true, that the amount of money spent on Y2K, yes, portions of it were sunk costs, but a large portion of it had a tremendous benefit. And Alan Greenspan has said to me, "I think the untold story of Y2K has been the upgrading of America's computer capability in the name of Y2K remediation that, in fact, produced a tremendous technological leap for which we will reap benefits for the years to come."

So if we follow the Koskinen model, as you suggest, of having someone constantly reminding the head of the agency that this is his or her responsibility—this is not the CIO's responsibility. This is not the IT people's responsibility. This is the secretary's responsibility. This is the administrator's responsibility. And John would have that experience. He would go to an agency, and they would say, "Well, you have come to fix Y2K," and he would say, "No, I haven't. You have to fix Y2K. I have come to monitor your efforts and report your efforts."

If we can get that going in the government, we will have the same response.

Now, I have asked GAO through my hat on the Joint Economic Committee for a report that is due October 15. Mr. Willemssen, I would assume you are involved in helping put that together. Can you give us any sense of whether we are going to be ready by October 15?

Mr. WILLEMSSEN. You will have a report on October 15, yes, sir.

Senator BENNETT. OK. I like——

Chairman LIEBERMAN. That is the right answer.

Senator BENNETT. I like that.

Now, mention has been made here about the Executive Order that is going to be issued. I have seen a copy of it. I assume the Chairman has as well. One of the things about that that I think we ought to focus on, Mr. Chairman, is the need for the ability of the Chairman of this effort to be able to testify before Congress. When we were talking about witnesses here, this was kind of a gray area, and the attitude was, well, it is the position of the White House that members of the White House staff don't testify. John Koskinen got around that because even though his title was Assistant to the President, the entire office was funded by the GSA. And, therefore, he was technically a GSA employee, regardless of what his title was. And, of course, if anybody has oversight over GSA, it is this Committee.

So I have had that conversation with people in the administration and said you ought to arrange it in such a way as to make it possible for the individual who is appointed as the chair of that effort within the administration to be able to come to the Congress, it will have a very beneficial effect on the relationships with the Congress.

So, simply reacting to your questions, I don't have a further question, but as I say, I love what you are saying because it coincides with the positions that I have taken.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Bennett. It is really great to have you involved in this based on all your experience with Y2K and all your other experience.

One of my staff members, just in response to what you said before about the possible use of automated systems in yesterday's tragedy, tells me that this morning on one of the networks there was an expert here saying that the precision with which the pilots hit the World Trade Center could have only been achieved through a computer system that allowed the pilots to input the exact coordinates of the World Trade Center and to have done so within a very short time of taking over the cockpit. This is hearsay, but it validates the point you raised in response to Senator Carper's question.

Senator BENNETT. If I could, Mr. Chairman, another piece of hearsay in response to Senator Carper, the plane that crashed presumably on the way to either Camp David or the Capitol had the transponder turned off manually in the cockpit. And, again, back to the point—this has nothing to do with the hearing, but you raised it and I think we ought to close the loop on it. Turning off the transponder that allows the air traffic controller to track the airplane is not an easy thing to do and it is not an obvious switch to find. So whoever did turn it off was well trained in cockpit procedures.

Chairman LIEBERMAN. One last question, going back to something you said very early in your testimony, Ms. Gross, that I was fascinated by but didn't understand was the possible desirability of laws to stop intrusions over cyberspace. Just develop that a bit more. You were talking about foreign intrusions, that is, intrusions that originate from abroad.

Ms. GROSS. Well, you never know exactly where they originate, but wherever they originate, once they come into the United States, there are a number of ports. Many of those ports are used for E-mail. They are used for other kinds of activity that is the normal use. But there are all these ports that are used for example for the system to test its own health. It is not a communication mechanisms.

Intruders come into those ports. They are called high ports. Those ports you can't banner and say, hey, this is a government computer, if you come in here we will monitor your keystrokes and stuff. Coming in the high port is like somebody coming in—instead of coming in your front door where people ring the bell and come in, is to come in through your chimney. Well, that is not a normal access route. These high ports are not normal access routes. The only ones that come in there are people that are going to do felonious activity. And yet it is not against the law from that to happen. There is not an anti-trespass act.

Chairman LIEBERMAN. Anti-trespass, OK. Understood.

Ms. GROSS. Yes. And that is a key bill. It has been talked about. The Department of Justice has talked about it. It has been proposed. I think that the FBI is pretty adamant on its need. It is one of the most crippling omissions for law enforcement being able to

do both the detection and the prosecution from a law enforcement point of view. High ports are used by hackers that are domestic and foreign. In our cases that we have seen where it looks like they have been coming in through various countries internationally, it is through those high ports. And the difficulty that we have in law enforcement, not system administrators, is there is no anti-trespass rule. It is a trespass for somebody to come into your house, and we don't have that law in cyberspace. And the laws have got to catch up with the 21st Century—the 20th Century, but now we are into the 21st Century.

Chairman LIEBERMAN. Yes, well said. I understand and appreciate it.

Senator CARPER. Just to follow up on that, you said it has been proposed but not enacted.

Ms. GROSS. Yes.

Senator CARPER. Has legislation been introduced in this Congress?

Ms. GROSS. It was introduced, I think, yes, in the DOD bill, just like GISRA was, the Government Information Security Reform Act. And I believe it got taken out.

Senator CARPER. Say that again? I am sorry.

Ms. GROSS. It was taken out of the defense authorization. I think Justice had been proposing it. It was winding its way through the Executive Branch and I don't believe they actually proposed it. It then became introduced in the Defense bill, and it never made it to the floor for final action.

There is no agency in law enforcement—there is uniform agreement. This is a key bill. You cannot talk to anybody in law enforcement that doesn't agree with that.

Senator CARPER. Would this be a good bill for Senators Lieberman, Bennett, and Carper to introduce?

Ms. GROSS. Absolutely.

Chairman LIEBERMAN. Let's do it.

Ms. GROSS. We liked GISRA.

Chairman LIEBERMAN. Are you sure that one wasn't coordinated, too? No, it sounds like a great idea. We should work together on it.

Thank you both. You have been superb, very thoughtful, substantive witnesses on a most pressing matter. I thank you and I would adjourn the hearing at this point.

[Whereupon, at 1 p.m., the Committee was adjourned.]

APPENDIX

Inspector General Reviews of Presidential Decision Directive 63 Implementation

Statement of

ROBERTA L. GROSS
Inspector General

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Before the

Senate Committee on Governmental Affairs

Hearing on "How Safe Is Our Critical Infrastructure?"

September 12, 2001

I. INTRODUCTION

As a nation, we have become more aware about the vulnerability of critical infrastructures, particularly to cyber attacks.[1] Just consider recent NewsBites published by the SANS (Security Administration, Networking and Security) Institute.[2]

- August 30, Invalid Worm: "The "Invalid" Worm arrives as an attachment purporting to be a patch from Microsoft." The worm mass mails itself to users and, once launched from an attachment, encrypts executable files rendering them unusable.

- August 31, Two Arrested in Encryption Device Export Plot: "A four month long investigation led to the arrest of two men who allegedly tried to smuggle

[1]Events such as the bombing of the Murrah Federal Building in Oklahoma City demonstrated that the Federal government needed to address new types of threats and vulnerabilities, many of which had not previously received a high priority. The Executive Branch formed a critical infrastructure working group, which included representatives from the defense, intelligence, law enforcement and national security communities. The working group identified both physical and cyber threats as growing concerns. For purposes of my testimony, I am focusing on the cyber critical infrastructure.

[2]SANS is a cooperative research and education organization founded in 1989 through which systems administrators, security professionals and network administrators share information and lessons learned.

encryption devices to China. The devices in question are designed for government use."

- August 31, British Business Group Wants Government Help With Cybercrime: "The UK's Confederation of British Industry (CBI) wants the government to take action against cybercrime by establishing a center for incident reporting and by updating the 1990 Computer Misuses Act to include attacks on computer systems. CBI says that the fear of financial losses due to cybercrime is preventing e-commerce from blossoming."

- August 29, Bank Replacing Compromised Debit Cards: "Three thousand Riggs Bank Customers will receive new Visa debit cards after an apparent breach of security on a server that processes Visa transactions. While no resulting instances of credit(sic) card fraud have been reported, the bank did not want to take any chances."

Investigations by the NASA Office of Inspector General (OIG) Computer Crimes Division (CCD) result in similar articles and headlines. For example, a joint investigation by NASA OIG computer crime sleuths, the Department of Defense Criminal Investigation Service, and the Federal Bureau of Investigation (FBI) resulted in a 16 year old juvenile from Miami, FL, being sentenced to 6 months in a detention facility. (This was the first time a juvenile computer hacker was sentenced to serve time.) The individual admitted to illegally accessing 143 computers at the Marshall Space Flight Center, Huntsville, Alabama. He obtained and downloaded proprietary software from NASA valued at approximately $1.7 million. The software supported the International Space Station's physical environments, including control of the temperature and humidity of the living space. The juvenile's actions required that the systems be shut down, which caused delivery delays of the program software. This resulted in additional costs of $41,000 in labor and equipment replacement. He also had illegally accessed Department of Defense computer networks and obtained more than 3,300 electronic messages and 19 user names and passwords. His intrusion specifically targeted a U. S. Army procurement system computer and copied and transferred a highly sensitive password file. This activity caused a costly computer shutdown and subsequent maintenance and restoration costs.

Clearly, juvenile hacker activity can be more than a mere nuisance!

In another recent investigation by the OIG CCD, a former NASA contractor employee and two others were sentenced for using NASA computer equipment to develop programs that allowed them to illegally capture ATM accounts and

Personal Identification Number (PIN) numbers to steal large sums of money from unsuspecting bank customers.

The harm caused by hackers is compounded because many hackers share their access with countless others by publicizing their exploits, tools and stolen passwords on Internet chat rooms. For example, OIG CCD agents, together with local law enforcement officials, arrested a hacker who illegally accessed a NASA computer system at one of NASA's research centers, obtained passwords and posted this information on the Internet.

The threats are also from international sources. Consider the following investigations conducted in parallel by the NASA OIG CCD and the FBI. In March 1998, CCD agents arrested one of the U. S. ringleaders of the Internet hacking group known as "ViRii". Our investigation revealed evidence about "ViRii" breaking into a large number of government, corporate, and university Internet-based systems. The NASA investigation into "ViRii" began in June 1997, when it became known that a NASA Jet Propulsion Laboratory (JPL) (Pasadena, CA) server was controlled and used by a number of U. S. and foreign hackers. The OIG CCD investigation identified the "ViRii" ringleader and others as possible suspects, including an Israeli national known as "Analyzer". In February 1998, separate attacks against other U. S. government sites caused the FBI and the Air Force Office of Special Investigations (AFOSI) to focus on "Analyzer". The FBI executed search warrants against two juveniles on February 25, 1998, in Cloverdale, California, to recover evidence of "Analyzer" related intrusions.

"Analyzer" is an Israeli citizen who was subsequently arrested in Israel based on evidence provided to Israeli authorities by a delegation of U. S. Federal Agents from Air Force Office of Special Investigations, FBI and the NASA CCD. The "ViRii" leader, the juvenile, and the Israeli all have been sentenced and/or adjudicated for their activities.

These examples demonstrate that network interconnectivity, while increasing productivity, clearly creates serious vulnerabilities.[3] The threats from the network even reach into our personal lives. The Internet exposes our very identities to theft when hackers steal vital information, including social security numbers, credit card numbers, etc. The NASA OIG has published a guide on preventing identity theft through computers in a brochure, "Protect Yourself and NASA Before Getting Rid of That Old Home Computer"

[3]Hackers can be insiders who are motivated by revenge, financial gain, and/or stress. External perpetrators are diverse, including teenagers showing off their skills; electronic protestors; terrorists; or possibly even foreign intelligence services.

(http://www.hq.nasa.gov/office/oig/hq/identify/html). Even simple acts of charity performed individually or as a government can be harmful (e.g., donating excess computers to organizations such as schools and prisons. Failure to properly and completely clear hard drives may expose confidential, sensitive, or proprietary information to unauthorized persons. The NASA OIG has issued several reports to NASA on this topic following inspections of excessed or surplused hard drives containing sensitive information. We also published a brochure widely distributed to the Agency, the IG community, and to Congress on the risks of carelessly excessing computers without sufficiently clearing hard drives. This brochure, "Clearing Information From Your Computer's hard Drive," is available at http://www.hq.nasa.gov/office/oig/harddrive.pdf.

II. PDD 63: ROLE OF INSPECTORS GENERAL[4]

The current Administration views securing the nation's critical infrastructure as a priority. The previous Administration established this priority through the issuance of Presidential Decision Directive 63 (PDD 63) on May 22, 1998. PDD 63 sets forth the mandate to protect our Nation's critical infrastructures[5] from acts that would significantly diminish the abilities of:

---

[4]Today's civilian Inspectors General (IGs), created by the Inspector General Act of 1978, as amended, independently review the programs and operations of their agencies; detect and prevent crime, fraud, waste, and abuse; and promote economy, efficiency and effectiveness so that their agencies can effectively serve the public. In simple terms, the IGs have three basic roles: to foster good program management, to prevent future problems, and deter, abate and punish crime and fraud.

IGs report both to the head of their respective agencies and to the Congress. This dual reporting responsibility is the framework within which IGs perform their functions. Unique in government, it is the legislative safety net that protects the IGs' independence and objectivity.

Collectively, during FY 2000, the IGs were responsible for:

- Potential savings of $9.5 billion.
- Recovery actions of almost $5.5 billion.
- More than 5,500 successful prosecutions.
- Suspensions or debarments of nearly 7,000 individuals or businesses.
- More than 2,600 civil or personnel actions.
- More than 120 testimonies before the Congress.

[5]PDD 63 defines critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government. . . . Many of the Nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked."

- the Federal government to perform essential national security missions and to ensure the general public health and safety;

- state and local governments to maintain order and to deliver minimum essential services; and

- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

PDD 63 assigns responsibilities to various groups, agencies and offices to achieve the protection of the Nation's critical infrastructure. Because of the importance of implementing this initiative, 21 agency and departmental (hereinafter agency) IGs agreed to review the progress by their agencies in carrying out their responsibilities to protect the nation's and their agencies' critical infrastructures. My office is coordinating this effort on behalf of the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE).[6]

As an aside, it is fitting that IGs are reviewing their agencies' infrastructure protection readiness. Since the Revolutionary War, military IGs have been tasked with independently reviewing the combat readiness of American troops. Today, the readiness needs of this nation call for different rules of engagement and the tools of future conflicts will be more diverse. PDD 63 was promulgated

---

[6]The IGs coordinate their professional activities through the PCIE and ECIE, which were established by Executive Order 12805. These councils work to promote collaboration on integrity, economy, and efficiency issues that transcend individual governmental agencies and to increase the professionalism and effectiveness of OIG personnel throughout the Government.

The PCIE is primarily comprised of the Presidentially appointed IGs and the ECIE is primarily comprised of IGs chosen and approved by heads of their agencies. The Deputy Director for Management of the Office of Management and Budget (OMB) chairs both Councils. Officials from the Federal Bureau of Investigation, Office of Government Ethics, Office of Special Counsel, and Office of Personnel Management serve on both Councils.

Recent projects by the Councils include:

- A Government-wide audit of non-tax delinquent debt ($46.4 billion at the time of the audit), which made a number of recommendations to enhance Federal debt collection.
- Special editions of *The Journal of Public Inquiry*, including a January 2001 issue to alert the new Administration to the key management challenges they would be facing.
- A Government-wide project to ensure Federal employee compliance with child support enforcement.
- Workshops on the implementation of the Government Information Security Reform (GISR), Title X, Subtitle G, of the 2001 Defense Authorization Act, approved October 30, 2000. See note 4, below.

as a step in implementing an adequate defense system for future potential conflicts.

The IGs are performing this important role in the infrastructure protection of the United States by establishing a Government-wide approach for assessing each agency's readiness for this critical challenge. The approach consists of four phases. Phase I relates to the adequacy of agency planning and assessment activities for protecting cyber-based infrastructures. Phase I has been completed and will be discussed below. Phase II, the review of the implementation of cyber plans, has been deferred to allow the agencies time to develop, implement, and evaluate their plans. Phase III, now in progress, will monitor agencies' planning and assessment activities related to critical physical structures. Phase IV will review the implementation of the plans related to the critical physical structures. We anticipate the completion of Phase III and the initiation of Phase II will occur sometime this Fall after the IGs forward their GISR reports related to their agencies' information security. The GISR effort complements PDD 63 activities.[7]

PDD 63 PHASE I REVIEW RESULTS:

On March 21, 2001, the PCIE/ECIE issued a report to the Honorable Mitchell E. Daniels, Jr., Director, Office of Management and Budget, reflecting generally the Phase I findings of the 21 participating OIGs. Our reviews summarized below, demonstrated collectively that the Federal Government can improve its PDD 63 planning and assessment activities for cyber-based critical infrastructures. It is, however, important to view these criticisms in the proper context; that is, because of the focus on critical infrastructure required by PDD 63, the nation is already in a better position because it is starting down the path towards a more robust effort to protect the Nation's critical infrastructure.

I will briefly highlight our collective findings in five areas:

- Misunderstanding of the applicability of PDD 63
- Imprecise performance measures
- Untimely identification of critical infrastructures
- Lack of coordinated management of PDD 63 requirements
- Failure to advance beyond the planning stage

[7]GISR primarily addresses the program management, implementation and evaluation of security related both to unclassified and national security systems. The Act directs IGs or their designees to perform annual independent evaluations of their respective agencies' information security programs and practices. The agencies, likewise, are required to submit an annual evaluation report to Congress. On September 10, 2001, each agency submitted a combined agency and IG report to OMB, summarizing IT security and related issues.

Applicability of PDD 63

Not all agencies began to implement PDD 63. Several agencies mistakenly believed that PDD 63 only applied to the specific agencies listed in the Directive and its addendum.[8] This misimpression was reinforced by an inaccurate interpretation by a key Federal player in overseeing the implementation of PDD 63. However, PDD 63 clearly applied to all agencies. PDD 63 Section VII, Protecting Federal Government Critical Infrastructures, provides,

> Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of the other aspects of that department's critical infrastructure. (Emphasis supplied.)

As a result of the misinterpretation, certain agencies did not prepare the required critical infrastructure plans and did not identify minimum essential infrastructures (MEIs). MEIs are defined as "the framework of critical organizations, personnel, systems and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes, essential to accomplishing an organization's core mission as they relate to national security, national economic security or continuity of government services". The agencies also did not perform vulnerability assessments of their MEI assets or develop remediation plans.

Most of the agencies that did not know PDD 63 applied to them began to address the Directive requirements as a result of the IG reviews.

Performance Measures

Agencies were told they were required to achieve a level of security preparedness, or "Initial Operating Capability" (IOC), no later than

---

[8]PDD 63 identified only certain agencies for specific tasks: Commerce – information and communications; Treasury – banking and finance; EPA – water supply; Transportation – aviation, highways (including trucking and intelligent transportation systems), mass transit, pipelines, rail; waterborne commerce; Justice/FBI – emergency law enforcement services; FEMA – emergency fire service, continuity of government services; HHS – public health services, including prevention, surveillance, laboratory services, and personal health services; Energy – electric power, oil and gas production and storage; Lead Agencies for Special Functions: Justice/FBI – law enforcement and internal security; CIA – foreign intelligence; State – foreign affairs.

December 31, 2000. However, agencies were not provided a uniform definition of IOC and so there was no consistent implementation. For example, one agency defined IOC to mean "completion of those initial mediation measures that are identified as needed by that time during the vulnerability assessment/ mitigation planning process." Representatives responsible for implementing PDD 63 in that agency said they could not understand the agency's definition of IOC. Another agency gave an entirely different definition of IOC: "(1) a broad level assessment of MEIs should be completed, (2) remediation plans should be completed for assets considered to be the most at risk, and (3) fixes should be in place for the most vulnerable assets." Without an adequate and consistent definition, the Federal Government can not adequately measure progress towards achieving full security preparedness.

Identification of Critical Infrastructure

At the time of the reviews, for a variety of reasons, most of the agencies which had submitted Critical Infrastructure Plans (CIPs)[9] had not identified and/or adequately identified their critical, cyber infrastructure assets. The reasons included lack of funds, poor methodology for identifying assets, and "higher priority" work.

The Executive Branch announced a standardized but non-mandatory process for identifying critical infrastructure assets entitled "Practices for Security Critical Information Assets." It also initiated Project Matrix, an ongoing effort that utilizes a multi-agency team evaluation to apply the Practices. Project Matrix involves a three-step process. In Step 1, the Project Matrix team identifies and prioritizes each agency's PDD 63-relevant assets. In Step 2, the the major nodes and networks upon which the most critical assets depend and identifies significant points of failure. In Step 3, the team identifies the infrastructure dependencies associated with select assets identified in Step 1 and analyzed in-depth in Step 2. The project Matrix guidance and process were not mandatory and generally had to be funded by the subject agency. Its success was limited by the amount of time and funds available to implement the process.

Management of PDD 63 Activities

The Federal organizations primarily responsible for implementing PDD 63 did not coordinate and manage their PDD 63 activities. The following

[9]PDD 63 requires that not later than 180 days from its issuance, every agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems.

organizations are among those responsible for coordinating and/or managing PDD 63 implementation:

- The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism is responsible for coordinating and implementing the Directive. The National Coordinator cannot direct departments and agencies but will ensure interagency coordination for policy development and implementation.
- The Office of Management and Budget is responsible for developing information security policies and overseeing agency practices.
- The National Institute of Standards and Technology is responsible for developing technical standards and providing related guidance for sensitive data.
- The National Security Agency is responsible for setting information security standards for national security agencies.
- The National CIAO, an interagency office, is responsible for developing an integrated National Infrastructure Assurance Plan to address threats to the Nation's critical infrastructure.
- The General Services Administration is the designated lead agency for the Federal sector.

The absence of coordinated oversight and management of PDD 63 has caused certain fundamental elements of the Directive to receive less than adequate attention.[10] As discussed earlier, several agencies had mistakenly decided not to implement PDD 63 because they believed, based in part on guidance from a key player in PDD 63 implementation, that they were exempt from the Directive.

Advancing Beyond the Planning Phase

Some agencies have not performed vulnerability assessments of their critical infrastructure assets or prepared the related remediation plans. This condition occurred because the budget requests that the agencies submitted to the OMB

[10]In April 2001, the U. S. General Accounting Office (GAO) submitted a report to the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U. S. Senate, "Critical Infrastructure Protection: Significant Challenges Developing National Capabilities (GAO-01-323). This report focused on the progress on the FBI's National Infrastructure Protection Center (NIPC) which, under PDD 63, had the role of providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings; facilitating and coordinating the law enforcement investigation on critical cyber infrastructure attacks. The GAO report noted the need for improvement in establishing information sharing partnerships between the NIPC and the private sector and other Federal Government agencies. The PCIE/ECIE group has not evaluated the NIPC's relationships with their agencies or the IG law enforcement community.

were rejected by OMB as not sufficiently detailed to justify funding the agencies' Critical Infrastructure Plans (CIPs) requirements.

The National Plan for Information Systems Protection, Version 1.0, "An Invitation to a Dialogue," acknowledged that the quality of the agencies' CIP budget requests did not meet OMB's expectations:

> Agency budget systems don't readily support collection of CIP data. Until these systems are modified, collection of information on CIP programs and budgets will be manual and inexact. The newness of CIP also means that the government is still on the steep part of a precipitous learning curve. Individual agencies are still grappling with the issue internally and the interagency process is still coming together. . . . When OMB issued its first CIP Budget Data Request (BDR) last year, it sought information at an activity level. But because of inadequate activity descriptions and data presentation problems, it was unable to consolidate the data, making it difficult to identify programmatic duplications and gaps that point up inconsistencies needing analysis and remedy. All this reduced confidence in the data.

III. NEXT STEPS

We made general suggestions to OMB based on our findings. Generally, these suggestions related to the need to better define terms, measures, and expectations set forth in PDD 63. Our suggestions also covered the need to ensure better coordination among the entities and organizations responsible for PDD 63 implementation.

We understand that in the very near future the White House will be issuing further guidance on protection of the nation's critical infrastructure. The PCIE/ECIE effort (coordinated by the NASA OIG) will play a part in this national effort by continuing the Government-wide review. This review will provide important feedback to heads of departments, OMB, other Executive entities, and the Congress. Also, individual IGs will have a vital role to play in the detection, deterrence, and prosecution of those committing cyber crimes against their victim agencies. With the Federal Government expanding e-government and e-commerce, the IGs necessarily will increase their criminal investigations in the cyberworld.

IV. CONCLUSION

PDD 63 provides an important focus on the Nation's critical infrastructure. The PCIE/ECIE found mixed progress in the Federal Government's implementation of this Directive. However, important steps have been taken. These steps must continue to ensure that our Nation has the capability to meet the growing threat of physical and computer-based attacks that potentially could cripple, disrupt and/or damage our critical infrastructure.

IGs have a unique role in assisting their agencies' critical infrastructure and planning implementation because of their ability to coordinate audits, inspections, and criminal investigation resources. They also will individually and collectively play a key role in the Nation's infrastructure protection through their reviews and cybercrime investigations.

United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs,
U.S. Senate

For Release on Delivery
Expected at
9:30 a.m. EDT
Wednesday,
September 12, 2001

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities

Statement of Joel C. Willemssen
Managing Director, Information Technology Issues

G A O
Accountability * Integrity * Reliability

GAO-01-1132T

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss efforts to protect federal agency information systems and our nation's critical computer-dependent infrastructures. Federal agencies, and other public and private entities, rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information.

Today, I will provide an overview of our recent reports on federal information security and critical infrastructure protection. Specifically, I will summarize the pervasive nature of federal system weaknesses, outline the serious risks to federal operations, and then detail the specific types of weaknesses identified at federal agencies. I will also discuss the importance of establishing a strong agencywide security management framework and how new evaluation and reporting requirements can improve federal efforts. Next, I will provide an overview of the strategy described in Presidential Decision Directive (PDD) 63 for protecting our nation's critical infrastructures from computer-based attacks. Finally, I will summarize the results of our recent report on the National Infrastructure Protection Center (NIPC), an interagency center housed in the Federal Bureau of Investigation (FBI), which is responsible for providing analysis, warning, and response capabilities for combating computer-based attacks.

RESULTS IN BRIEF

Because of our government's and our nation's reliance on interconnected computer systems to support critical operations and infrastructures, poor information security could have potentially devastating implications for our country. Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk. In particular, federal agencies continue to have deficiencies in their entitywide security programs that are critical to their success in ensuring that risks are understood and that effective controls are selected and implemented. The new information security provisions that you, Mr. Chairman,

and Senator Thompson originally introduced as legislation will be a major catalyst for federal agencies to improve their security program management. To help maintain the momentum that the new information security reform provisions have generated, federal agencies must act quickly to implement strong security program management.

A key element of the strategy outlined in PDD 63 was establishing the NIPC as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. The NIPC has initiated a variety of critical infrastructure protection efforts that establish a foundation for future governmentwide efforts. However, the analytical and information-sharing capabilities that PDD 63 asserts are needed to protect the nation's critical infrastructures have not yet been achieved. We made various recommendations to the Assistant to the President for National Security Affairs and the Attorney General regarding the need to more fully define the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with private-sector and federal entities. To improve our nation's ability to respond to computer-based incidents, the administration should consider these recommendations as it reviews how the government is organized to deal with information security issues.

BACKGROUND

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups. In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency

services all depend on the security of their computer operations. Likewise, the speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

Reports of attacks and disruptions are growing. The number of computer security incidents reported to the CERT Coordination Center® (CERT-CC)[1] rose from 9,859 in 1999 to 21,756 in 2000. For the first 6 months of 2001, 15,476 incidents were reported. As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A potential hacker can literally download tools from the Internet and "point and click" to start a hack. According to a recent National Institute of Standards and Technology publication, hackers post 30 to 40 new tools to hacking sites on the Internet every month.

Recent attacks over the past 2 months illustrate the risks. These attacks, referred to as Code Red, Code Red II, and SirCam, have affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. They have already reportedly caused billions of dollars of damage, and their full effects have yet to be completely assessed. Code Red attacks have reportedly (1) caused the White House to change its website address, (2) forced the Department of Defense (DOD) to briefly shut down its public websites, (3) infected Treasury's Financial Management Service causing it to disconnect its systems from the Internet, (4) caused outages for users of Qwest's high-speed Internet service nationwide, and (5) delayed FedEx package deliveries. Our testimony last month provides further details on the nature and impact of these attacks.[2]

These are just the latest episodes. The cost of last year's ILOVEYOU virus is now estimated to be more than $8 billion. Other incidents reported in 2001 illustrate the problem further:

---

[1]CERT Coordination Center® is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[2]*Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* (GAO-01-1073T, August 29, 2001).

- A hacker group by the name of "PoizonB0x" defaced numerous government web sites, including those of the Department of Transportation, the Administrative Office of the U.S. Courts, the National Science Foundation, the National Oceanic and Atmospheric Administration, the Princeton Plasma Physics Laboratory, the General Services Administration, the U.S. Geological Survey, the Bureau of Land Management, and the Office of Science & Technology Policy. (Source: Attrition.org., March 19, 2001.)

- The "Russian Hacker Association" offered over the Internet an e-mail bombing system that would destroy a person's "web enemy" for a fee. (Source: UK Ministry of Defense Joint Security Coordination Center.)

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, or degrade the integrity of and deny access to data.[3] As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood that information attacks will threaten vital national interests increases. In addition, the disgruntled organization insider is a significant threat, since such individuals with little knowledge about computer intrusions often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets.

[3]These terms are defined as follows: *Virus*: a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bombs*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

WEAKNESSES IN FEDERAL SYSTEMS REMAIN PERVASIVE

Since 1996, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September 1996, we reported that serious weaknesses had been found at 10 of the 15 largest federal agencies, and we concluded that poor information security was a widespread federal problem with potentially devastating consequences.[4] In 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies; both analyses found that all 24 agencies had significant information security weaknesses.[5] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[6]

Our most recent analysis, last April, of reports published since July 1999, showed that federal computer systems continued to be riddled with weaknesses that put critical operations and assets at risk.[7] Weaknesses continued to be reported in each of the 24 agencies covered by our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented, (2) access controls, which ensure that only authorized individuals can read, alter, or delete data, (3) software development and change controls, which ensure that only authorized software programs are implemented, (4) segregation of duties, which reduces the risk

[4] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).
[5] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).
[6] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); *High-Risk Series: An Update* (GAO/HR-99-1, January 1999); *High Risk Series: An Update* (GAO-01-263, January 2001).
[7] *Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk* (GAO-01-600T, April 5, 2001).

that one individual can independently perform inappropriate actions without detection, (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse, and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

Our April analysis also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. While these increases in reported weaknesses are disturbing, they do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits covered in our analysis were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as DOD and the Department of Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of systems supporting nonfinancial operations. In response to congressional interest, during fiscal years 1999 and 2000, we expanded our audit focus to cover a wider range of nonfinancial operations. We expect this trend to continue.

RISKS TO FEDERAL OPERATIONS ARE SUBSTANTIAL

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not

impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections, and weaknesses at DOD increase the vulnerability of various military operations. Further, information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure. For example, in 1999, a Social Security Administration employee pled guilty to unauthorized access to the administration's systems. The related investigation determined that the employee had made many unauthorized queries, including obtaining earnings information for members of the local business community.

More recent audits in 2001 show that serious weaknesses continue to be a problem and that critical federal operations and assets remain at risk.

- In August, we reported that significant and pervasive weaknesses placed the Department of Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.[8] Also, Commerce's inspector general has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.[9]

---

[8] *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk* (GAO-01-751, August 13, 2001).

[9] *Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements*, Inspector General Audit Report No. FSD-12849-1-0001.

- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than $12 billion annually in payments that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.[10]

- In March, we reported that although the DOD's Department-wide Information Assurance Program had made progress in addressing information assurance, it had not yet met its goals of integrating information assurance with mission readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.[11]

- In February, the Department of Health and Human Services' Inspector General again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[12] Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which was responsible, during fiscal year 2000, for processing more than $200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data, such as Medicare enrollment, eligibility and paid claims data, and to process all payments for managed care.

---

[10] *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk* (GAO-01-615, July 3, 2001).
[11] *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, March 30, 2001).
[12] *Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000*, A-17-00-00014, February 26, 2001.

Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

These types of risks, if inadequately addressed, may limit the government's ability to take advantage of new technology and improve federal services through electronic means. For example, this past February, we reported on serious control weaknesses in the Internal Revenue Service's (IRS) electronic filing system, noting that failure to maintain adequate security could erode public confidence in electronic filing, jeopardize the Service's ability to meet its goal of 80 percent of returns being filed electronically by 2007, and deprive it of financial and other anticipated benefits. Specifically, we found that, during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both within and outside IRS, could have gained access to these systems and viewed, copied, modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electronic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS completed corrective action for all the critical access control vulnerabilities we identified before the 2001 filing season and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.[13] As part of our audit follow up activities, we plan to evaluate the effectiveness of IRS' corrective actions.

Addressing weaknesses such as those we identified in the IRS's electronic filing system is especially important in light of the administration's plans to improve government services by expanding use of the Internet and other computer-facilitated operations—collectively referred to as electronic government, or E-government.[14] Specific initiatives proposed for fiscal year 2002 include expanding electronic means for (1) providing information to citizens, (2) handling procurement-related transactions, (3) applying for and managing federal grants, and (4) providing citizens information on the development of specific federal rules and regulations.

[13] *Information Security: IRS Electronic Filing Systems* (GAO-01-306, February 16, 2001).
[14] *The President's Management Agenda, Fiscal Year 2002* www.whitehouse.gov/omb/budget.

Anticipated benefits include reducing the expense and difficulty of doing business with the government, providing citizens improved access to government services, and making government more transparent and accountable. Success in achieving these benefits will require agencies and others involved to ensure that the systems supporting E-government are protected from fraud, inappropriate disclosures, and disruption. Without this protection, confidence in E-government may be diminished, and the related benefits never fully achieved.

CONTROL WEAKNESSES ACROSS AGENCIES ARE SIMILAR

Although the nature of agency operations and their related risks vary, striking similarities remain in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. Likewise, similarities exist in the corrective actions they must take. The following sections describe the six areas of general controls and the specific weaknesses that were most widespread at the agencies covered by our analysis.

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost effective manner rather than reacting to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed security plans for major systems based on risk (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on ineffective controls, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they execute. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Also, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and departing employees, as well as changes in users' responsibilities and related access needs.

Significant access control weaknesses were reported for all the agencies covered by our analysis, as shown by the following examples:

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled nor were they adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, at one agency, former employees and contractors could still and in many cases did read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.
- Users were not required to periodically change their passwords.
- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At another agency, 20,000 users had been provided access to one system without written authorization.
- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the ability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also, at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate network vulnerability testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to

sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. Our auditors have been successful, in almost every test, in readily gaining unauthorized access that would allow both internal and external intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. Also, much of the activity associated with our intrusion testing has not been recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Software Development and Change Controls

Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and ensure that different versions are not misidentified.

Such controls can prevent errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that, depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Weaknesses in software program change controls were identified for almost all the agencies for which these controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and

were operating effectively. At another agency, documentation was not retained to demonstrate user testing and acceptance.

- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs was prevented or detected.
- Agencies' policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or
- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Segregation of

duties can be enforced by a combination of physical and logical access controls and by effective supervisory review. We identified weaknesses in segregation of duties at most agencies covered by our analysis. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff members involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 staff members had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt-recorded by the same individual.

Operating System Software Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals

might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosure. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. Weaknesses were identified at each agency for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Further, pervasive vulnerabilities in network configuration exposed agency systems to attack. These vulnerabilities stemmed from agencies' failure to (1) install and maintain effective perimeter security, such as firewalls and screening routers, (2) implement current software patches, and (3) protect against commonly known methods of attack.

Service Continuity Controls

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should

interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity control weaknesses were reported for most of the agencies covered by our analysis. Examples of weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.
- Disaster recovery plans were not fully tested to identify their weaknesses. For example, periodic walkthroughs or unannounced tests of the disaster recovery plan had not been performed. Conducting these types of tests provides a scenario more likely to be encountered in the event of an actual disaster.

SECURITY PROGRAM MANAGEMENT CAN BE IMPROVED WITH NEW EVALUATION AND REPORTING REQUIREMENTS

The audit reports cited in this statement and in our prior information security reports include many recommendations to individual agencies that address specific weaknesses in the areas I have just described. It is each individual agency's responsibility to ensure that these recommendations are implemented. Agencies have taken steps to address problems, and many have remedial efforts underway. However, these efforts will not be fully effective and lasting unless they are supported by a strong agencywide security management framework.

Establishing such a management framework requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). Our study found that these organizations managed their information security risks through a cycle of risk management activities that included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet these needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

In addition, a strong, centralized focal point can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computing environments.

Implementing this cycle of risk management activities is the key to ensuring that information security risks are adequately considered and addressed on an ongoing, agencywide basis. Included within it are several steps that agencies can take immediately. Specifically, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. Although none of these actions alone will ensure good security, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay.

Due to concerns about the repeated reports of computer security weaknesses at federal agencies, in 2000, you, Mr. Chairman, and Senator Thompson introduced government information security reform legislation to require agencies to implement the activities I have just described. This legislation was enacted in late 2000 as part of the fiscal year 2001 National Defense Authorization Act. In addition to requiring security program management improvements, the new provisions require that both management and agency inspectors general annually evaluate agency information security programs. The Office of Management and Budget (OMB) has asked agencies to submit the results of their program reviews and the results of their inspector general's independent evaluation this week. In accordance with the new law, OMB plans to develop a summary report to the Congress later this year. This summary report, and the subordinate agency reports, should provide a more complete picture of the status of federal information security than has previously been available, thereby providing the Congress and OMB with an improved means of overseeing agency progress and identifying areas needing improvement.

This annual evaluation and reporting process is an important mechanism, previously missing, for holding agencies accountable for implementing effective security and managing the problem from a governmentwide perspective. We are currently reviewing agency implementation of the new provisions.

CRITICAL INFRASTRUCTURE PROTECTION EFFORTS SUPPLEMENT TRADITIONAL INFORMATION SECURITY

Beyond the risks of computer-based attacks on critical federal operations, the federal government has begun to address the risks of computer-based attacks on our nation's computer-dependent critical infrastructures, such as electric power distribution, telecommunications, and essential government services. Although these efforts pertain to many traditional computer security issues, such as maintaining the integrity, confidentiality, and availability of important computerized operations, they focus primarily on risks of national importance and encompass efforts to ensure the security of privately controlled critical infrastructures.

The recent history of federal initiatives to address these computer-based risks includes the following.

- In June 1995, a Critical Infrastructure Working Group, led by the Attorney General, was formed to (1) identify critical infrastructures and assess the scope and nature of threats to them, (2) survey existing government mechanisms for addressing these threats, and (3) propose options for a full-time group to consider long-term government responses to threats to critical infrastructures. The working group identified critical infrastructures, characterized threats to them, and recommended creating a commission to investigate such issues.

- In February 1996, the National Defense Authorization Act required the executive branch to provide a report to the Congress on the policies and plans for developing capabilities to defend against computer-based attacks, such as warnings of strategic attacks against the national information infrastructure.[15] Later that year, the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs, began to hold hearings on security in cyberspace. Since then, congressional interest in protecting national infrastructures has remained strong.

[15]National Defense Authorization Act of Fiscal Year 1996, Pub. L.104-106, Div. A, Title X, Subtitle E, Section 1053.

- In July 1996, in response to the recommendation of the 1995 working group, the President's Commission on Critical Infrastructure Protection was established to further investigate the nation's vulnerability to both cyber and physical threats.

- In October 1997, the President's Commission issued its report,[16] which described the potentially devastating implications of poor information security from a national perspective.

In response to the commission's report, the President initiated actions to implement a cooperative public/private approach to protecting the nation's critical infrastructures by issuing PDD 63 in May 1998. The directive called for a range of activities to improve federal agency security programs, establish a partnership between the government and private sector, and improve the nation's ability to detect and respond to serious attacks. The directive established critical infrastructure protection as a national goal, stating that, by the close of 2000, the United States was to have achieved an initial operating capability and, no later than 2003, the capability to protect the nation's critical infrastructures from intentional destructive acts.

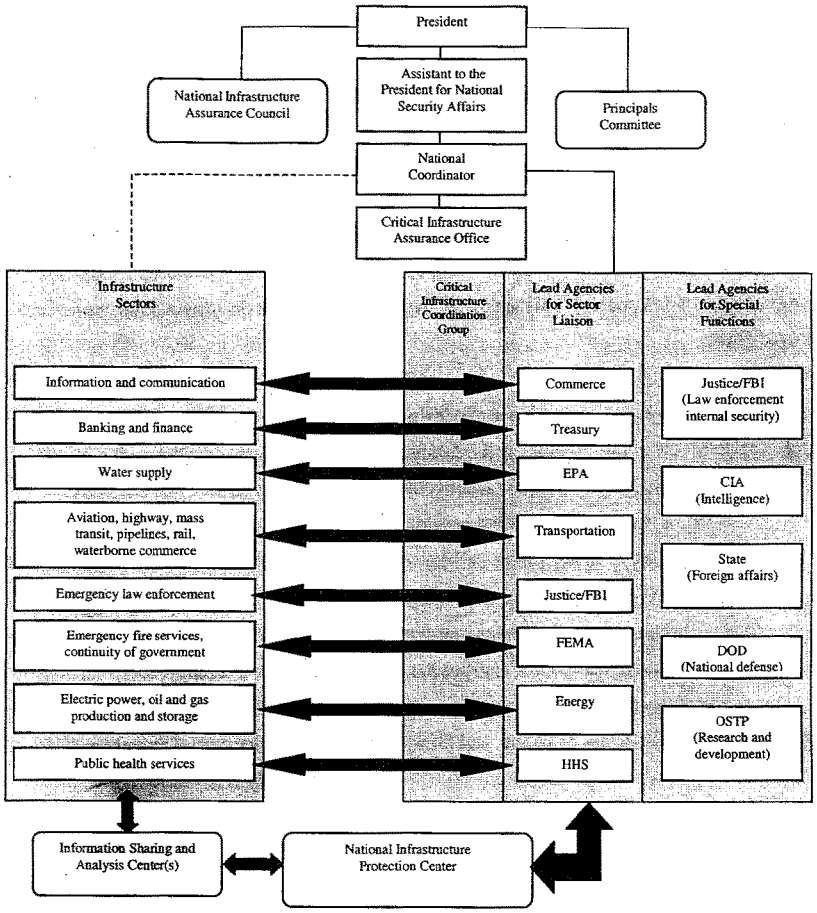
To accomplish its goals, PDD-63 designated the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who reports to the Assistant to the President for National Security Affairs, to oversee the development and implementation of national policy in this area. The directive also established the National Plan Coordination staff, which became the Critical Infrastructure Assurance Office, an interagency office housed in the Department of Commerce responsible for planning infrastructure protection efforts. It further authorized the FBI to expand its National Infrastructure Protection Center (NIPC) and directed the NIPC to gather information on threats and coordinate the federal government's response to incidents affecting infrastructures.

In addition, the directive designated "lead agencies" to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and

[16]*Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection,* October 1997.

the Department of Energy is responsible for working with the electric power industry. Similarly, regarding special function areas, DOD is responsible for national defense, and the Department of State is responsible for foreign affairs. To facilitate private-sector participation, PDD 63 encouraged the creation of Information Sharing and Analysis Centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the NIPC. Figure 1 depicts the entities with critical infrastructure protection responsibilities as outlined by PDD 63.

Figure 1: Critical Infrastructure Protection Responsibilities as Outlined by PPD 63



Source: The Critical Infrastructure Assurance Office.

Shortly after the initial issuance of PDD 63, we reported on the importance of developing a governmentwide strategy that clearly defines and coordinates the roles of new and existing federal entities to ensure governmentwide cooperation and support for PDD 63. [17] Specifically, we noted that several of PDD 63's provisions appeared to overlap with existing requirements prescribed in the Paperwork Reduction Act; OMB Circular A-130, Appendix III; the Computer Security Act; and the Clinger-Cohen Act. In addition, some of the directive's objectives were similar to objectives being addressed by other federal entities, such as developing a federal incident handling capability, which was then in the process of being addressed by the National Institute of Standards and Technology and the federal Chief Information Officers Council.[18] At that time, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the Assistant to the President for National Security Affairs ensure such coordination.

In July 2000, we reported that a variety of activities had been undertaken in response to PDD 63, including developing and reviewing individual agency critical infrastructure protection plans, identifying and evaluating information security standards and best practices, and the White House's issuing its *National Plan for Information Systems Protection*[19] as a first major element of a more comprehensive strategy to be developed.[20] At that time, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.

---

[17] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

[18] The federal incident handling program is now operated by the Federal Computer Incident Response Center at the General Services Administration.

[19] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue,* The White House, January 7, 2000.

[20] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination* (GAO/T-AIMD-00-268, July 26, 2000).

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in PDD 63. On May 9, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and reviewing how the government is organized to deal with information security issues.

NIPC PROGRESS HAS BEEN MIXED

A key element of the strategy outlined in PPD 63 was the establishment of the NIPC as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned the NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing.

In April, we reported on the NIPC's progress in developing national capabilities for analyzing threat and vulnerability data and issuing warnings, responding to attacks, and developing information-sharing relationships with government and private-sector entities.[21] Overall, we found that while progress in developing these capabilities was mixed, the NIPC had initiated a variety of critical infrastructure protection efforts that had laid a foundation for future governmentwide efforts. In addition, the NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical and information-sharing capabilities that PDD 63 asserted are needed to protect the nation's critical infrastructures had not yet been achieved, and the NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

[21] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

Multiple Factors Have Limited Development of Analysis and Warning Capabilities

PDD 63 assigns the NIPC responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent.

Since its establishment in 1998, the NIPC has issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. These analyses have included (1) situation reports related to law enforcement investigations, including denial-of-service attacks that affected numerous Internet-based entities, such as eBay and Yahoo, and (2) analytical support of a counterintelligence investigation. In addition, the NIPC has issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

The use of strategic analysis to determine the potential broader implications of individual incidents has been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

Three factors have hindered the NIPC's ability to develop strategic analytical capabilities.

- First, there is no generally accepted methodology for analyzing strategic cyber-based threats. For example, there is no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.

- Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because other federal agencies have not provided the originally anticipated number of detailees. For example, at the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of the NIPC's 3-year existence. In addition, the NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.
- Third, the NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work in February, only three industry assessments had been partially completed, and none had been provided to the NIPC.

To provide a warning capability, the NIPC established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. As of February, the unit had issued 81 warnings and related products since 1998, many of which were posted on the NIPC's Internet web site. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. The NIPC's ability to issue warnings promptly is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

However, I want to emphasize a more fundamental impediment in the NIPC's progress that echoes our previously reported concerns about the need for a more clearly defined critical infrastructure protection strategy. Specifically, evaluating its progress in developing analysis and warning capabilities was difficult because the entities involved in the government's critical infrastructure protection efforts did not share a common interpretation of the NIPC's roles and responsibilities. Further, the relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National

Security Council were unclear regarding who has direct authority for setting NIPC priorities and procedures and providing NIPC oversight. In addition, its own plans for further developing its analytical and warning capabilities were fragmented and incomplete. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

In our April report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data,
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources, and
- clearly define the role of the NIPC in relation to other government and private-sector entities.

In commenting on a draft of the report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council stated that our report highlighted the need for a review of the roles and responsibilities of the federal agencies involved in U.S. critical infrastructure protection support. In addition, he stated that the administration will consider our recommendations as it reviews federal cyber activities to determine how the critical infrastructure protection function should be organized. The Special Assistant to the President added that some functions might be better accomplished by distributing the tasks across several existing federal agencies, creating a "virtual analysis center" that would provide not only a governmentwide analysis and reporting capability, but that could also support rapid dissemination of cyber threat and warning information.

NIPC Coordination and Technical Support Have Benefited Investigative and Response Capabilities

PDD 63 directed the NIPC to provide the principal means of facilitating and coordinating the federal government's response to computer-based incidents. In response, the NIPC undertook efforts in two major areas: providing coordination and technical support to FBI investigations and establishing crisis-management capabilities.

First, the NIPC provided valuable coordination and technical support to FBI field offices, that established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for the NIPC field squads and teams.

While these efforts benefited investigative efforts, FBI and NIPC officials told us that increased computer capacity and data transmission capabilities would improve their ability to promptly analyze the extremely large amounts of data that are associated with some cases. In addition, FBI field offices were not yet providing the NIPC with the comprehensive information that NIPC officials say is needed to facilitate prompt identification and response to cyber incidents. According to field office officials, some information on unusual or suspicious computer-based activity had not been reported because it did not merit opening a case and was deemed to be insignificant. To address this problem, the NIPC established new performance measures related to reporting.

Second, the NIPC developed crisis-management capabilities to support a multiagency response to the most serious incidents from the FBI's Washington, D.C., Strategic Information Operations

Center. From 1998 through early 2001, seven crisis-action teams had been activated to address potentially serious incidents and events, such as the Melissa virus in 1999 and the days surrounding the transition to the year 2000, and related procedures have been formalized. In addition, the NIPC coordinated the development of an emergency law enforcement plan to guide the response of federal, state, and local entities.

To help ensure an adequate response to the growing number of computer crimes, we recommended in our April report that the Attorney General, the FBI Director, and the NIPC Director take steps to (1) ensure that the NIPC has access to needed computer and communications resources and (2) monitor the implementation of new performance measures to ensure that field offices fully report information on potential computer crimes to the NIPC.

Progress in Establishing Information-Sharing Relationships Has Been Mixed

Information sharing and coordination among private-sector and government organizations are essential for thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as we testified in July 2000,[22] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

NIPC's success in this area has been mixed. For example, the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, was viewed by the NIPC as an important element in building trust relationships with the private sector. As of January 2001, the InfraGard program had grown to about 500 member organizations, and, recently, NIPC officials told us that InfraGard membership has continued to increase. However, of the four information sharing and analysis centers that had been established as focal points for infrastructure sectors, a two-way, information-sharing partnership with the NIPC had developed with only one—the electric power industry. The NIPC's dealings with two of the other three centers primarily consisted of providing information to the centers without

[22] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation* (GAO/T-AIMD-00-268, July 26, 2000). Testimony before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives.

receiving any in return, and no procedures had been developed for more interactive information sharing. The NIPC's information-sharing relationship with the fourth center was not covered by our review because the center was not established until mid-January 2001, shortly before the close of our work. However, according to NIPC and ISAC officials, the relationships have improved since our report.

Similarly, the NIPC and the FBI made only limited progress in developing a database of the most important components of the nation's critical infrastructures—an effort referred to as the Key Asset Initiative. Although FBI field offices had identified over 5,000 key assets, at the time of our review, the entities that own or control the assets generally had not been involved in identifying them. As a result, the key assets recorded may not be the ones that infrastructure owners consider the most important. Further, the Key Asset Initiative was not being coordinated with other similar federal efforts at DOD and the Department of Commerce.

In addition, the NIPC and other government entities had not developed fully productive information-sharing and cooperative relationships. For example, federal agencies have not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's Federal Computer Incident Response Center. Further, NIPC and Defense officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. According to the NIPC director, the relationship between the NIPC and other government entities has improved since our review. In recent testimony, officials from Federal Computer Incident Response Center and the U.S. Secret Service discussed the collaborative and cooperative relationships between their agencies and the NIPC.

The NIPC has been more successful in providing training on investigating computer crime to government entities, which is an effort that it considers an important component of its outreach efforts. From 1998 through 2000, the NIPC trained about 300 individuals from federal, state,

local, and international entities other than the FBI. In addition, the NIPC has advised several foreign governments that are establishing centers similar to the NIPC.

To improve information sharing, we recommended in our April report that the Assistant to the President for National Security Affairs

- direct federal agencies and encourage the private sector to better define the types of information necessary and appropriate to exchange in order to combat computer-based attacks and to develop procedures for performing such exchanges,
- initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, and
- resolve discrepancies in requirements regarding computer incident reporting by federal agencies.

We also recommended that the Attorney General task the FBI Director to

- formalize information-sharing relationships between the NIPC and other federal entities and industry sectors and
- ensure that the Key Asset Initiative is integrated with other similar federal activities.

In commenting on a draft of this report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council said that the administration will consider our recommendations as it reviews federal cyber activities to determine how the critical infrastructure protection function should be organized.

- - - - -

In conclusion, efforts are underway to mitigate the risks of computer-based attacks on federal information systems and on our national computer dependent infrastructures. However, recent reports and events indicate that these efforts are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks.

The evaluation and reporting requirements of the new Government Information Security Reform provisions should help provide a more complete and accurate picture of federal security weaknesses and a means of measuring progress. In addition, it is important that the government ensure that our nation has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damage to our critical infrastructures. The analysis, warning, response, and information-sharing responsibilities that PDD 63 assigned to the NIPC are important elements of this capability. However, developing the needed capabilities will require overcoming many challenges. Meeting these challenges will not be easy and will require clear central direction and dedication of expertise and resources from multiple federal agencies, as well as private sector support.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have at this time. If you should have any questions later about this testimony, please contact me at (202) 512-6253. I can also be reached by e-mail at willemssenj@gao.gov.

(310136)

United States General Accounting Office September 2001

GAO
Accountability * Integrity * Reliability

Highlights

CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities

Highlights of GAO-01-1132T, testimony to the Committee on Governmental Affairs, U.S. Senate

Why GAO Did This Study

GAO has designated information security as a governmentwide high-risk area since 1997 because of growing evidence that controls over computerized federal operations and our nation's critical infrastructures were not effective and because the related risks were escalating, in part, due to increasing reliance on the Internet.

Since poor information security could have such potentially devastating implications for our country, GAO continues to assess, and make recommendations to improve, our nation's ability to deal with the growing threat of computer-based attacks.

What GAO Recommends

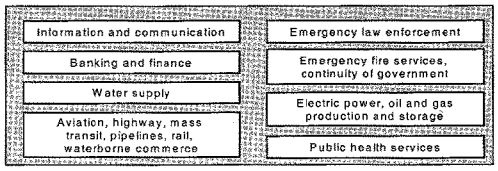
GAO has made numerous recommendations to agencies regarding pervasive weaknesses and steps to take to develop strong security program management.

As for critical infrastructure protection, GAO made several recommendations* to the Assistant to the President for National Security Affairs and the Attorney General regarding the need to more fully define the role and responsibilities of the National Infrastructure Protection Center, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with private-sector and federal entities.

What GAO Found

Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, GAO's expanded body of audit evidence shows that federal computer security continues to be fraught with weaknesses and that, as a result, critical operations and assets continue to be at risk. In particular, federal agencies continue to have deficiencies in their entitywide security programs. Such programs are critical to agencies' success in ensuring that risks are understood and that effective controls are selected and implemented. Recently enacted information security legislation can be a major catalyst for federal agencies to improve their security program management. By acting on the momentum of these provisions to develop strong program management, federal agencies will increase the likelihood of their success in dealing with the growing threat of computer-based attacks.

Beyond the risks of computer-based attacks on individual federal agency operations, a presidential directive outlined a governmentwide strategy to address the risks of these attacks on our nation's computer-dependent critical infrastructures. A key element of this strategy was establishing the FBI's National Infrastructure Protection Center as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. As noted in a recent GAO report,* the Center had initiated various critical infrastructure protection efforts. However, the analytical and information-sharing capabilities that the directive asserts are needed to protect the nation's critical infrastructures had not yet been achieved. Developing these needed capabilities will not be easy and will require clear central direction and dedicated expertise and resources from multiple federal agencies, as well as support from the private sector.



Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities (GAO-01-323, April 25, 2001).

This is a test for developing highlights for a GAO report. The full testimony is available at www.gao.gov/cgi-bin/getrpt?GAO-01-1132T. For additional information about the testimony, contact Joel C. Willemssen (202) 512-6253. To provide comments on this test highlights, contact Keith Fultz (202-512-3200) or email HighlightsTest@gao.gov.

Testimony and Statement for the Record of Christopher Darby, CEO, @stake, Inc., Peiter Zatko, Chief Scientist and VP of Research & Development, @stake, Inc., and Chris Wysopal, Director of Research & Development, @stake, Inc.

Hearing on "How Secure is Our Critical Infrastructure?" before the Committee on Governmental Affairs

United States Senate

Wednesday, September 12, 2001
Room 342, Dirksen Senate Office Building

@stake Inc. is the world's largest independent digital security consulting and engineering firm. Formed in 1999, @stake today works with more than 100 clients worldwide including many Fortune 1000 financial and telecommunications institutions. Over the past two years @stake has gathered over 100 of the world's leading authorities on digital security including people from the NSA, DERA (the U.K. equivalent of the NSA), the FBI, RSA Security, Nortel, MIT, Certco and other prominent institutions. @stake today staffs operations throughout the United States and in Europe.

Three years ago Mssrs. Zatko and Wysopal, then members of the L0pht security think tank, testified before this committee on the subject of, "Weak Computer Security in Government." Today the focus has expanded to encompass the national critical infrastructure, recognizing that government security is dependant on the security of many entities outside of government, for the most part for-profit enterprises.

@stake's business model has not, to date, focused on the Government. Our focus has been on the large commercial enterprises. Many of our clients provide services in support of critical national infrastructure. The majority of @stake's client engagements focus on assessing digital risks and engineering technical solutions for large multinational companies. It must be remembered that the mandate for these companies is to derive shareholder return, not to secure critical infrastructure. Today @stake's client base views security as a sunk cost, largely a byproduct of Information Technology architecture and associated spending. Security is viewed as a cost borne to mitigate risks that may negatively impact the corporate mandate of generating shareholder return.

The following testimony provides opinion on the security of our national critical infrastructure, specifically as it depends upon the security strategy, architecture and implementation of large commercial enterprises providing such things as financial, telecommunication, energy, and transportation services.

History

Three years ago attention was drawn to risks taken with technologies that were not well understood. Technologies were being deployed without regard to the larger purpose of the organization. Businesses and government were driving full steam ahead to exploit the potential of Internet technologies. Although the Internet had tremendous resilience and potential, it was of no concern that there were still vulnerabilities serious enough to bring the whole thing crashing down. People involved in understanding offensive security research could, to use a now famous line, "take down the Internet in 30 minutes." What was referred to then were weaknesses in central points in the network, and the use of mechanisms similar to the now well known distributed denial of service attacks.

The proposed solution to the computer security problem was to get vendors and infrastructure owners to take security more seriously, by forcing them to find the weaknesses and problems in their own products. To this effort people endeavored to publicly educate vendors in ways of finding and attacking problems in software and network systems. Fundamental changes in the way vendors and businesses approach security was required.

The Changing Threat Model

Today's threat model is not addressed by simply running the most popular firewall. Today's threat model is not addressed by access control. These components look only at a myopic section of the risk. The fact is today's threat is no longer about active attack. Today's threat is about passive control. Yesterday's elite hacker is today's puppetmaster, no longer content to deface or disrupt a website, but instead seeking total information control. The world of application security has only just become visible on the horizon as a huge area of risk that has not attempted to protect itself.

Recent worms such as Code Red, while gaining notoriety, pale in comparison to similar, though lesser known worms, that lie dormant with the capability of manipulating the nation's critical infrastructure under their master's control. To illustrate the potentially catastrophic nature of this threat consider that an estimated one third of the classified data on SIPRNET now relies upon these public shared infrastructures.

The threat model has indeed changed. A multi-disciplinary emphasis of strategic and tactical must be embraced. With the majority of the world attacking security as a tactical response, we must now compensate with more strategic thinking if we are to successfully move into the next era.

Strategic Architectural Design

Security policies and security mechanisms should, but unfortunately often do not, vary greatly from one organization to another. Too often due-diligence is viewed as the

installation of protective software in it's "out of the box" configuration. A university has very different security requirements than a bank or a utility company. Different levels of risk demand different amounts and types of risk mitigation. @stake has found that the level of security varies greatly even within organizations in the same industry. This is especially disturbing when the organizations are part of our nation's critical infrastructure where information security requirements are the highest.

This is more pronounced in areas such as electrical utilities and gas refineries. These are potentially enticing targets in the new world threat model. Both business models understand and utilize a segmentation structure around what is called Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS). These systems are vulnerable to attack and could potentially disrupt the operations supporting infrastructure such as the national power grid.

As security consultants, @stake gets to see the details of the security architectures of many organizations. Recently we looked at the information security design of two critical infrastructure organizations, a large modern oil refinery and that of a large fossil fuel power plant. The contrast was stark.

The refinery was highly automated with many sensors and computer controlled machines and a succinct network design. There were multiple levels of firewalls to protect the many different security levels. Information was only allowed to pass in one direction: from the most sensitive levels where the computer controlled devices were connected, up to a less sensitive network, the plant control network, and then finally to the least sensitive network, the corporate network, which is where you would find standard business operations like accounting.

The network design grew out of performance, reliability and safety concerns but had the added benefit of being very secure. Since information could only flow in one direction on the network it was not possible for someone on the corporate network to affect the sensitive computer controlled devices running the refinery. The network was designed so that someone, perhaps in accounting, couldn't make a mistake and query a piece of equipment for historical data, which might impact the performance of the equipment if it was contacted at the wrong time. This same design protects the sensitive plant equipment from being controlled by a malicious attacker who may have broken into the corporate network from the Internet or from a malicious insider in the corporate offices.

The fossil fuel power plant was a completely different story. The different network levels at the power plant were all joined together without a firewall to segment them from one another. The plant network was connected to the corporate network with a simple network router that did not provide adequate network filtering. The end result was that anyone, anywhere on the corporate network for this very large power company could control this power plant and perhaps many others. The only thing stopping anyone on the Internet from wreaking havoc with the power plant was a single level of firewall that separated the power company's corporate network from the Internet. In the case of critical infrastructure this is clearly not good enough.

How did two similar industrial computer networks end up being implemented so differently? The answer lies in the way they were put together. The power plant network grew over time in an ad hoc way. Pieces were added one by one as technology became available without an overall network architecture. The refinery network had a strict architecture that had to be adhered to, as the network was built. It is like the difference between a planned community and a shantytown. Planning has many benefits: reliability, performance and security. You can often achieve better performance and more functionality without upfront planning but to achieve the proper security, especially the level required for critical infrastructure, it must be planned in from the start.

Security of commercial software

Vendors have responded to the onslaught of publicly reported vulnerabilities in their products by shortening the time their response teams took to fix problems once the problem was reported. While software security is conceded to time to market pressures, companies appear willing to expend more energy in reacting rather than proper design. The notion of proactively analyzing code in anticipation of future attack situations has been entirely overlooked.

The path of reactive fixes or "patches" to software requires customers to expend effort installing them on every machine that has the vulnerability. Ironically today most organizations have not realized that part of their total cost of ownership for a piece of software is the monthly installation of patches. In organizations with tens of thousands of computers, this maintenance cost greatly affects their bottom line.

Microsoft's web server, a core component of many businesses today, illustrates this trend. In 1998 there were 5 software patches released for it, in 1999 there were 10, in 2000 there were 16, and through August 2001 there have been 6. Microsoft is not alone in this regard. All of the major vendors approach software security in this way.

A full month before the Code Red worm, Microsoft provided a solution that, if it had been installed correctly, would have mitigated the risks resulting from the Code Red attack. At the height of the Code Red worm infestation there were several hundred thousand machines that had been compromised. Even today after many weeks and a lot of media attention there are still an estimated 40,000 unpatched and vulnerable computers that remain infected.

The majority of organizations that configured their internal software to use only those components required to meet their business needs would not have been vulnerable to the Code Red worm. @stake consultants are constantly editing out unnecessary functionality to assist client's in streamlining their operations and enhancing their security profile. They often do not even have to worry about the vendor supplied patch.

The ultimate goal is to architect for maximum performance while minimizing complexity.

How does one prepare for the future rather than patching the past? The Code Red worm could have been much worse. Had this worm been written correctly, the steps used to mitigate its attack on whitehouse.gov would have been ineffective. By theorizing solutions about the logical evolution of this type of worm, our defense and security goals can be better realized. In the words of Winston Churchill – the worst-case scenario should never come as a surprise.

Education

Reacting to today's environment will lead to defenses that are incapable of protecting against tomorrow's threat. Understanding current and future attack methodologies is the important first step of defensive computer security research. By fully exploring anticipated attack methodologies and attack tool capabilities, defenders will be placed ahead of attackers. The Department of Defense acknowledged it is building prototype biological weapons. In order to best come up with defenses against biological weapons, researchers first had to build prototype weapons in order to understand their capabilities. Only then could they start to model defense methods. Information weapons have much in common with biological weapons as they both allow small groups to inflict severe and widespread damage and attack with no warning.

People need to understand and be educated to the security risks. Security and technical people need to learn how to communicate in a language that is understood by both the technical and business constituencies. A technical person needs to communicate to a business executive in the business terms relative to the organizations goals. Conversely, a business person needs to convey business goals to the engineers.

Tools and threat models will invariably change over time. A security mindset is required. This mindset recognizes that a tool is only one component of the larger solution. A solution must evolve on an ongoing basis to anticipate and meet the emerging threats. In short, security education is an ongoing process and security solutions must be living.

Hidden Threats

Island hopping

One of the new significant threats to both the government and the commercial sector is "island hopping." Island hopping is the act of automatically scanning large ranges of network addresses (often dedicated to servicing personal, or home users) and taking control of the remote user's computer. This tactic results in attackers taking control of the unsuspecting user's computer in order to then "hop" into the user's corporate network, utilizing the victims own VPN to bypass the corporate firewall.

Cable modem, DSL, and dial-up Internet Service Providers have large blocks of address spaces from which they dynamically assign addresses to users who connect and disconnect on demand. These addresses are scanned looking for vulnerabilities in common operating systems and applications. No longer is the threat the network, it is now the application.

Breaching an organization's perimeter remains the goal. The avenue of attack has shifted to the weakest link, the employee's home computer. In this example, the VPN is converted into an attack tool as opposed to a security solution.

Few organizations have the resources or awareness to bring each employee's personal system up to the same security level as the organizational firewall. This is the same system that children play network games on, home banking is engaged in, and unrestricted web surfing and online chat occur. This same home computer is being trusted, via the VPN, to enter the corporate perimeter and appear in tandem on the "secure" network. Island hopping compromises as many systems as possible in an automated fashion and then looks for systems that have VPN interfaces configured giving them access to the internal networks of agencies and organizations.

A large software giant on the west coast suffered a significant attack and the resulting loss of critical assets in exactly this fashion. What would have happened if the Leaves worm (a malignant worm active today and designed to be controlled by one or more unidentified individuals), which was estimated to have compromised over 200,000 systems, had been instructed to report which systems were trusted as internal through VPNs? @stake estimates that the majority of organizations in the private and public sector, would have had their firewalls by-passed.

The Leaves worm ingeniously piggybacked itself onto another remote control program called Sub7. Finding previously compromised computers and taking control of them was just the beginning of what made Leaves interesting. The real interesting fact was that a single person controlled all of the computers infected with Leaves by using a public chat network called IRC or Internet Relay Chat.

This worm was created to control as many computers as possible. Once a computer was under its control it could launch a denial of service attack on a piece of the Internet, be a launching point to spread other new worms, or anything else the "puppetmaster" could dream up in the future. Just by issuing a few simple commands over the IRC chat system he could get his army of computers to do his bidding.

Over the past 3 years attack and control technologies have steadily advanced but the primary defensive technologies, firewalls and antivirus scanners, have remained mostly the same. They are in more widespread use but have not stepped up to solve the problems that hit the Internet at its weakest point, vulnerabilities in applications and operating systems. Attack technologies such as worm toolkits, multiplatform worms, polymorphic shell code, and kernel level root kits, make it possible for attackers to compromise more computers, faster, and remain in control of those computers. Routers,

which control the flow of network information, are also the targets of many of these control networks.

Wireless Technology

In the past, attackers monitoring President Clinton's whereabouts by intercepting secret service pages demonstrated the lack of security in deployed wireless technologies. Attempts to introduce security to these existing technologies is mediocre at best. Unfortunately, the lessons learned have not been applied to the new wireless technologies.

Technology is adopted at a pace that exceeds the time period needed to responsibly vet it. A case in point is wireless networking. Within the last year there has been a tremendous growth in the installations of a wireless networking standard popular with corporate and small office users called 802.11b. It only costs about $100-200 per computer to install and allows the computer to use the corporate network and usually the Internet at high speed without being wired. The problem is installing this technology without planning to do it securely for your environment opens up a corporate network to easy attack. This attack can be launched by outsiders in the parking lot armed with little more than a laptop. Informal surveys of major cities, taken by individuals conducting an activity known as "war driving", have shown that over 60% of the networks discovered do not employ even minimum security precautions. Even when the security settings in wireless networks are enabled, an attacker can bypass the security because of flaws in the network and security standards themselves.

This wireless technology is so convenient that even defense contractors, who should be acutely aware of the need for security, have found their employees installing wireless equipment and putting their networks at risk. In June of this year, MITRE, a federally funded research and development center that performs work for the Defense Department, found that anyone could access their internal network from their parking lot. The corporate vulnerability was due to the ad hoc wireless networks many employees had installed without considering the risks it posed to their organization.

Today's Internet does not require a central authority to oversee additional equipment or applications being added to a network. This has an adverse effect. Unless rigorous policies are in place and enforced by regular audits, vulnerabilities will be created as new technology is added without investigating its impact to the organization. MITRE now has a policy forbidding wireless networks to be deployed without the permission of their information technology group.

Multi-disciplinary devices

When Secretary of State Colin Powell announced he would no longer be using his Palm Pilot, a popular Personal Digital Assistant (PDA), for security concerns, it surprised

many people. Not too much later Hanson, the FBI agent found guilty of selling secrets to Russia, was arrested and found to have been outfitted with a customized PDA to help him in his nefarious tasks. Do these events signify an inherent problem with PDA's? No. Most PDA's are great for what they were originally designed for. Storing notes, phone numbers, recipes, and acting as a handy calculator are all great for personal convenience. The problem arises when boundaries between different disciplines become blurred or erased. In this case the two disciplines being crossed are that of personal life and professional. One security paradigm seldom encompasses both worlds without impacting or affecting either.

How many people use the same password on personal devices as they do on critical systems? It is unreasonable to believe that the same amount of effort is placed to secure devices found in personal use as those deployed within Critical Infrastructure. However, these devices are freely used between and betwixt both arenas. While the crossing of a social boundary is quite apparent to most people, the crossing of security boundaries is much less apparent while potentially much more disastrous.

Application Security

An Achilles heel of Critical Infrastructure is vulnerabilities within applications. Firewall technology has done a good job of thwarting many network style attacks and blocking access to computers that have not been configured properly for security. However, applications such as a web servers, email programs, and word processors handle the data and communicate with other programs over the network to do their job. This communication cannot be blocked by a firewall or the program ceases to function. These communications give access to the critical data.

Attackers employ primitive, yet effective, tactics to reverse engineer popular programs to discover new vulnerabilities. They can then compromise the security of a computer by sending specially crafted messages or commands to the newly vulnerable application. This is frequently the modus operendi of worms and those who seek to control and harness armies of computers through automated attacks.

There is no simple solution for this problem such as installing a firewall or antivirus software. Each application must undergo rigorous testing to find its latent vulnerabilities, which are typically the result of design or implementation errors.

The bad guys already have the proprietary source code to most operating systems and applications. This includes the operating systems that run on routers, the backbone of the Internet. This gives them a huge advantage in discovering latent vulnerabilities. Source code is the target for many computer intrusions. When Microsoft's corporate network was pierced in October, 2000 it was source code for upcoming products that was stolen. Kevin Mitnick bragged that he broke into Motorola to steal the source code for their products. The stockpiling and trading of source code over the Internet is a daily activity in the computer underground.

The source code for proprietary operating systems such as Windows NT/XP/2000, Solaris, HP/UX, Cisco IOS, Cisco PIX, Firewall-1, and others swapped like baseball cards between attackers. This is why it is so important that third party security audits of software not be hampered by anti-reverse engineering restrictions. Again, the reality is the bad guys already have the source code.

Our organization was forced to create a way to derive the equivalent of source code from the binary applications run on end systems. Our tools represent today's thought leadership in the area of application security analysis. Attempts are being made to restrict access to this type of technology but the fact is attackers are actively pursuing equivalent data. It is our belief that in only a few years time it will similarly be possible for the rest of the world to have total visibility into the applications that support our nations critical infrastructure.

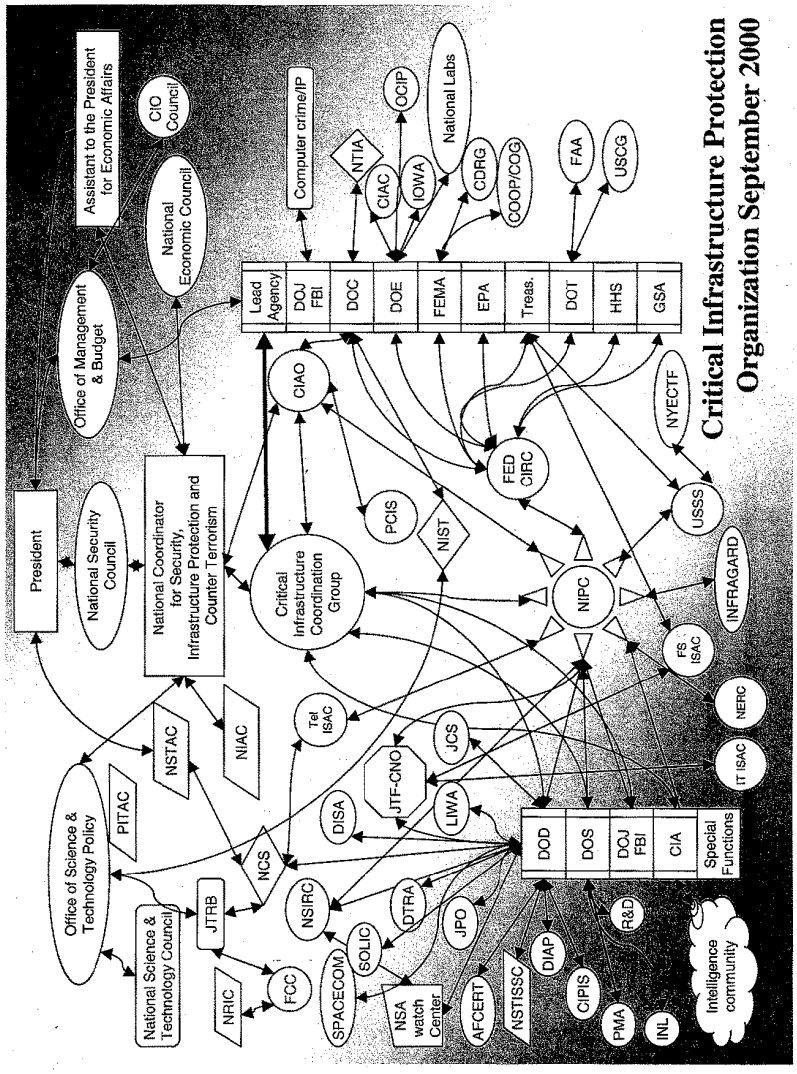
Conclusion

There are significant new and emerging cyber threats to the critical infrastructure of the Untied States. Perhaps the most disturbing of these new threats are those that lie dormant, awaiting instruction from unknown persons. While it is beyond the scope of this testimony to imply motive on the part of these persons, it is reasonable to assume that substantial damage could result from inappropriate use of the hijacked infrastructure.

The software industry has not taken appropriate measures to ensure the security of commercial code. The problems are further compounded by inefficient implementation and a lack of security education. In an ideal world, software would be analyzed and secured against emerging threat models prior to release to the market. Today's reality, however, is rooted in reactive tactics aimed at mitigating financial risk as opposed to physical attack.

It is also disturbing to observe that a false sense of security is being propagated in the search for a "silver bullet." Strong tools such as anti-virus software, firewalls and VPNs do not, in themselves, solve the security issues. These tools provide limited assistance in securing against core software or hardware vulnerabilities.

Education coupled with persistent analysis of emerging threat models and the corresponding solutions is the only answer.


Critical Infrastructure Protection
Organization September 2000
President
National Security Council
National Coordinator for Security, Infrastructure Protection and Counter Terrorism
Office of Management & Budget
Assistant to the President for Economic Affairs
National Economic Council
CIO Council
Office of Science & Technology Policy
National Science & Technology Council
PITAC
NSTAC
NIAC
JTRB
NRIC
FCC
NCS
NSIRC
SOLIC
SPACECOM
NSA watch Center
AFCERT
NSTISSC
DIAP
CIPIS
PMA
R&D
INL
Intelligence community
DTRA
JPO
DISA
JTF-CNO
LIWA
JCS
Tel ISAC
Critical Infrastructure Coordination Group
CIAO
PCIS
NIST
FED CIRC
NIPC
USSS
NYECTF
FS ISAC
NERC
IT ISAC
INFRAGARD
Lead Agency
DOJ FBI
DOC
DOE
FEMA
EPA
Treas.
DOT
HHS
GSA
Computer crime/IP
NTIA
CIAC
IOWA
OCIP
National Labs
CDRG
COOP/COG
FAA
USCG
DOD
DOS
DOJ FBI
CIA
Special Functions